McNAIR PAPER 62

The Revenge of the Melians: Asymmetric Threats and the Next QDR

KENNETH F. McKENZIE, JR.

Institute for National Strategic Studies
National Defense University

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2000	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Revenge of the Melians: Asymmetric Threats and the Next QDR	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Kenneith F. /McKenzie, JR	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
National Defense Univesrity Institute for National Strategic Studies Fort McNair Washington, DC 20319	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**118**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

About the Author

Lieutenant Colonel Kenneth F. McKenzie, Jr., USMC, is a senior military fellow in the Institute for National Strategic Studies at the National Defense University, where he is a member of the Quadrennial Defense Review 2001 Working Group. Prior to this assignment, he commanded the 1st Battalion, 6th Marines, which deployed to the Mediterranean as the Ground Combat Element of the 24th Marine Expeditionary Unit. LtCol McKenzie also served as a platoon commander, rifle company commander, infantry battalion executive officer, and division operations officer, among other assignments. He also has been the Marine Officer Instructor at the Virginia Military Institute and a speechwriter for the Commandant's Staff Group at U.S. Marine Corps Headquarters.

LtCol McKenzie is a graduate of The Citadel, where he earned a bachelor's degree in English and master's in history. He was graduated with honors from the advanced course at the U.S. Army Armor School, is a distinguished graduate of the Marine Corps Command and Staff College, and is a recipient of the Clifton B. Gates Award from the School of Advanced Warfighting at Marine Corps University.

■ ■ ■ ■

The National Defense University (NDU) is a joint professional military education institution operating under the direction of the Chairman of the Joint Chiefs of Staff. Its purpose is to prepare military and civilian leaders for service at the highest levels of national defense and security. The principal operating elements of NDU are the Industrial College of the Armed Forces, National War College, Armed Forces Staff College, Information Resources Management College, Institute for National Strategic Studies, and Center for Hemispheric Defense Studies.

The Institute for National Strategic Studies (INSS) conducts strategic studies for the Secretary of Defense, Chairman of the Joint Chiefs of Staff, and unified commanders in chief; supports national strategic components of NDU academic programs; and provides outreach to other governmental agencies and the broader national security community.

The Publication Directorate of INSS publishes books, monographs, reports, and occasional papers on national security strategy, defense policy, and national military strategy through National Defense University Press that reflect the output of university research and academic programs. In addition, it produces *Joint Force Quarterly*, a professional military journal published for the Chairman of the Joint Chiefs of Staff.

The Revenge of the Melians: Asymmetric Threats and the Next QDR

Kenneth F. McKenzie, Jr.

McNair Paper 62

INSTITUTE FOR NATIONAL STRATEGIC STUDIES
NATIONAL DEFENSE UNIVERSITY
WASHINGTON, D.C.
2000

For sale by the U.S. Government Printing Office. To order, contact
Superintendent of Documents, Mail Stop: SSOP, Washington, D.C. 20402–9328
(SSN 1071–7552)

Contents

Foreword vii

Introduction ix

Chapter One
What is Asymmetric Warfare? 1
Defining Asymmetry—Characteristics: Disparity of Interest—Targeting the Will of the Opponent—Attaining Strategic Effect on All Levels of War—The Importance of Effectiveness—The Threat-Response Dynamic—A Final Example: The Gulf Tanker War—Conclusions

Chapter Two
A Typology of Asymmetry: What, Who, and When? 19
The What: The Range of Potential Asymmetric Threats—The Who: Regional, Rogue, and Nonstate Actors—The When: Likelihood During Phases of a Crisis—Conclusions

Chapter Three
Looking in the Mirror: Where Are Our Asymmetric Vulnerabilities? 55
Measuring Conventional Military Superiority—Examining the Homeland—Quantifying the Homeland: What Are the Targets?—Examining Potential Vulnerabilities

Chapter Four
Categorizing the Threats 65
What Are the Ten Asymmetric Threats?—Conclusions

Chapter Five
An Option of Difficulties—Countering Asymmetric Threats 81
Current Initiatives: The State of Play Today—Summarizing Current Initiatives—Doing Better: Beginning with Three Ideas—Policy Recommendations—An Option of Difficulties?

Chapter Six
Conclusions: The Uneasy Athenians 95

Endnotes 97

List of Tables

1. Asymmetric opportunities 3

2. Conventional antideployment approaches 43

3. Conventional anti-invasion approaches 45

4. Summarizing antiaccess measures 47

5. A question of timing: relative likelihood of asymmetric use during phases of a crisis 52

6. Measuring the effectiveness of *JV 2010* concepts and some potential asymmetries 59

7. What's the homeland? Breaking it out 61

8. Summary of ten asymmetric threats 79

Foreword

This essay is a product of the Quadrennial Defense Review (QDR) 2001 Working Group, a project of the Institute for National Strategic Studies at the National Defense University. Sponsored by the Chairman of the Joint Chiefs of Staff, the working group is an independent, honest-broker effort intended to build intellectual capital for the upcoming QDR. More specifically, it aims to frame issues, develop options, and provide insights for the Chairman, the services, and the next administration in three areas: defense strategy, criteria for sizing conventional forces, and force structure for 2005–2010.

One of the group's initial tasks was to assess the future security environment to the year 2025. This was pursued by surveying the available literature to identify areas of consensus and debate and by deepening knowledge of asymmetric threats to the United States both at home and abroad, given their potential appeal to likely adversaries in view of America's conventional military superiority. The essay that follows grew out of that latter effort and reflects a growing consensus that the issues posed by asymmetric threats should occupy a more prominent place in defense strategy and force planning.

This essay makes a unique contribution to the growing literature on asymmetric threats by providing a conceptual framework for thinking about such threats, offering an approach to determining which threats should receive the greatest attention from defense planners, and suggesting concrete steps that the Nation should take to address them.

Michèle A. Flournoy
Project Director

Introduction

In 416 B.C., the Athenian-led Delian League, then the dominant naval power of the Hellenic World, was locked in a death struggle with its rival, Sparta, and its Peloponnesian allies. In the wake of the battle of Mantinea, and on the eve of the ill-fated naval expedition to Syracuse, the small island of Melos in the northern Cretan Sea had become an object of strategic concern to Athens which sought to force Melos to join the Delian League and pay tribute. The Melians refused and claimed the moral right of a state to remain neutral."Right, as the world goes, is only in question between equals in power," answered the Athenians; "The strong do what they wish and the weak suffer what they must."[1]

One may admire Melian principles and courage, if not strategic acumen. Their heroic stubbornness cost the Melians their existence. The Athenians slaughtered all adult males and sold the women and children into slavery.

The Melian Dialogue by Thucydides, an account of the exchange recorded between the Athenian negotiators and the Melians, has been a *locus classicus* for the realistic study of international relations for millennia—especially the notorious Athenian refusal to be constrained by the unenforceable dicta of hypothetical international law. Weak states have long sought to counter the overwhelming political, economic, and military superiority that great powers can bring to bear. Melos, treading a familiar path, sought succor against one power through an alliance with another, Sparta, which failed.

Absent a powerful ally, the most effective responses from weaker states have been those that sought to counter the hegemon's power indirectly through superior military organization, crafty diplomacy, wily espionage, or terror. Modern counterparts of the Melians can add weapons of mass destruction with a long reach to this traditional arsenal.

The Melians might have survived, had they been able to raise the cost to the Athenians of attacking their island. Weak nations today can do what Melos could not—inflict severe damage on attacking forces or a distant homeland. As weak nations, and even nonstate groups, contemplate intimidating or punishing a dominant power on a scale inconceivable 2,500 years ago, we might speak metaphorically of the revenge of the Melians and hear far-distant applause of those islanders.

Indeed, in the aftermath of the Cold War, Americans are in some sense the modern analogues to the ancient Athenians. Because the United States is the world's strongest power, it is inevitable that hostile nations will seek ways to undermine its great strength by asymmetrically attacking its vulnerabilities.

The central thesis of this essay is that the ability of the Department of Defense to execute its portion of U.S. national policy in the near to mid-term is based on the *ability to maintain clear and unambiguous conventional military superiority in the face of emerging asymmetric threats*, coupled with *the ability to defend the homeland*.[2] Today, the interest of the defense establishment in asymmetric threats is nothing more than a modern recognition of an enduring truth: weaker powers, both state and nonstate, will relentlessly seek ways to mitigate the dominance of the strong.

This analysis will adopt a three-part approach to analyzing asymmetric threats:

- What is asymmetric warfare?
- What are the asymmetric threats we face?
- What can we do to counter asymmetric threats?

This introduction will establish the broad framework for the subsequent analysis. Chapter one will attempt to answer the question "what is asymmetric warfare?" What does the term mean? More particularly, what does it signify for the defense establishment? In establishing this relationship, current definitions of asymmetric warfare will be examined, and a more nuanced concept will be proposed. Five characteristics of asymmetric warfare will be introduced. As part of chapter one, illustrative asymmetric approaches will be examined within their historical and operational contexts. Finally, some conclusions about measures of effectiveness for different asymmetric approaches will be advanced.

Chapter two will begin the process of answering the second question by posing a typology of asymmetric approaches and organizing the current range of asymmetric threats facing the United States. This chapter

will build upon the historical analysis of chapter one, but will turn its focus to contemporary and future threats. Chapter three will operationalize the range of potential asymmetric threats by comparing potential asymmetric threats against two systems: the operational principles embodied in *Joint Vision 2010* and the critical infrastructure of the United States. In chapter four, the range of asymmetric threats will be evaluated in terms of potential danger, and threats likely to pose the greatest danger will be identified.A series of future case studies are included in this chapter to give a sense of immediacy and granularity to the threats.

Chapter five represents the policy component of this study. This chapter will evaluate current United States initiatives against asymmetric threats, assessing the effectiveness of existing policy. A set of specific policy recommendations will then be advanced for consideration during the 2001 Quadrennial Defense Review. Some of these will be outside the purview of the Department of Defense, requiring action across the Federal Government, as well as by state and local governments.

Before we begin this analysis, we must address the skeptic's question: is the new found lure of asymmetric warfare nothing more than defense faddism? This is a reasonable suspicion given the rapidity with which this term has sprung up and spread within defense circles. Is there, in other words, *less* here than meets the eye?

It will become apparent in the following pages that increased attention to asymmetric warfare is justified and timely. Throughout history, nations in conflict have attempted to take advantage of the weaknesses of their adversaries while maximizing their own strengths to achieve a disproportionate effect—one of the characteristics of what we now call asymmetric warfare. This study, however, recognizes a new aspect of the asymmetric dimension of war; that the incontestable global conventional military superiority of the United States, coupled with the proliferation of weapons of mass destruction and the death of strategic distance, have made the Armed Forces uniquely vulnerable to asymmetric threats.

Chapter One

What is Asymmetric Warfare?

. . . victories not of resources but of strategic doctrine: the ability to break the framework which had come to be taken for granted and to make the victory all the more complete by confronting the antagonist with contingencies which he had never considered.[3]

—Henry A. Kissinger, *Nuclear Weapons and Foreign Policy*

This chapter will establish a working definition of asymmetric warfare by examining current definitions, then proposing a variant that will be applied throughout the rest of this study. Five recurring characteristics that are useful in analyzing asymmetric approaches also will be introduced as themes that resonate throughout the rest of the paper, with historical examples to highlight different aspects of both successful and unsuccessful asymmetric approaches.

Defining Asymmetry

The use of the term *asymmetric warfare* is new in U.S. Government circles. It does not appear in the 1990 Base Force, the 1993 Bottom-Up Review, the 1995 Commission on Roles and Missions of the Armed Forces, or any annual Secretarial Report to the congress until 1998.[4] In fact, the first mention of the term was in the 1997 Quadrennial Defense Review (QDR) report.[5] Since then, the asymmetric threat industry has been rocketing ahead. The National Defense Panel that shadowed the QDR effort, the 1999 U.S. Commission on National Security/21st Century, and a host of other analyses have since weighed in on its significance.[6] The National Defense University, in the 1998 edition of its annual *Strategic Assessment,* devoted an entire chapter to asymmetric threats, whereas in previous volumes the term had never been mentioned. The term figured large

in the Secretary's Report in 1999.[7] The concept also made an appearance with the publication of the *National Military Strategy* in 1997 for the first time, and also in the *National Security Strategy*.[8] The 1999 Joint Strategy Review, an internal analytical study prepared annually for the Chairman, focused on the asymmetric threat.[9]

The U.S. military's working definition of asymmetric warfare says that "adversaries are likely to attempt to circumvent or undermine U.S. strengths while exploiting its weaknesses, using methods that differ significantly from the usual mode of U.S. operations."[10] A recent Joint Staff definition opines that asymmetric warfare consists of "unanticipated or non-traditional approaches to circumvent or undermine an adversary's strengths while exploiting his vulnerabilities through unexpected technologies or innovative means."[11]

In December 1999, *A National Security Strategy for a New Century*, the fundamental national security document of the United States, defined asymmetric warfare in this manner: "unconventional approaches that avoid or undermine our strengths while exploiting our vulnerabilities."[12]

The existing definitions, while narrowly accurate, seem insufficient in explaining asymmetry. It will be argued in this chapter that a better definition of asymmetric warfare would be: *Leveraging inferior tactical or operational strength against American vulnerabilities to achieve disproportionate effect with the aim of undermining American will in order to achieve the asymmetric actor's strategic objectives.* The key differences in this proposed definition are the element of *disproportionate effect*—achieving strategic objectives through application of modest resources—and the explicit recognition of the importance of the *psychological* component. These elements are essential to considering how an asymmetric actor can achieve strategic objectives through an operation—even a failed operation—that, from the perspective of the larger power, is only a tactical attack.

There is an important caveat to this definition: asymmetric warfare does not equate automatically to an attack on the homeland. Unfortunately, much recent attention in the literature has tended to obscure the fact that asymmetric approaches exist on all levels of war, and forces in the field as well as nations have been seeking them for as long as warfare and diplomacy have been practiced. The attack on the homeland is only the most extreme—and potentially most dangerous—expression of an asymmetric strategic attack.

Characteristics: Disparity of Interest

Any consideration of asymmetric threats must start with the most basic asymmetry of all: disparity of interest. The matrix below highlights the fact that the greatest incentive for using asymmetric approaches rises from a real or perceived disparity of interest. When a weak adversary has a vital interest that conflicts with the nonvital interest of a strong state, the former has the greatest incentive to use asymmetric approaches.

Given the breadth of American security interests, there will be many areas of potential conflict where no vital interest is at stake for the United States, but where a regional actor has vital interests. We should remember that a rich man's small-scale contingency may be a poor man's major theater war. The greatest chance for success for an adversary in such a scenario is when U.S. interest remains relatively low.

Table 1. Asymmetric opportunities

	Adversary interest is nonvital	Adversary interest is vital
U.S. interest is **nonvital**	Lowest incentive for both sides	Most effective opportunity for adversary use of asymmetric approaches
U.S. interest is **vital**	Low incentive for weaker side	Most dangerous situation

Asymmetric approaches can work in three ways within this idea. First, they can deter U.S. entry into crises where there is no U.S. vital interest by threatening disproportionate damage to the United States. Would the loss of Seattle to a ballistic missile attack be a reasonable trade for the unconditional surrender of a hostile Pyongyang government? Absent a vital American interest, such a threat would exercise a powerful sobering effect on U.S. planners. This is probably the most effective illustration of this concept, and also the most likely to have a positive outcome for the weaker state.

Second, if a decision has been made to employ U.S. forces in a contingency that nonetheless remains below the level of vital national interest, an asymmetric approach by an adversary that threatens to rapidly cause disproportionate effect may halt U.S. entry, or accelerate a withdrawal. If

the perceived U.S. stake is low, and if it becomes apparent that involvement may become very expensive in terms of human and material cost, then a weaker state might calculate that a shocking display of force might cause the United States to recalculate the cost-benefit of engagement.

Third, an asymmetric approach may enable regional actors to pursue aggressive strategies indirectly, making it hard to marshal American will to act. Information operations, terrorist attacks, and other unconventional approaches all may tend to make it very difficult to trace sponsorship with the certainty required by the United States for action, ultimately diffusing our response until it may be too late to act effectively. To this end, regional states will work very hard to "manage" their relationship with the United States, while pursuing dual goals of attaining regional objectives and preventing our interference.

Does this mean that it is advantageous to be weak? Intriguingly, the Melian Dialogue offers a paradoxical twist for modern times. The final measure between the Melians and the Athenians was the ability of the Athenians to apply unconstrained power against their weaker adversary; this is no longer the case. The nature of international relations, and the approach of free societies to war, limits—properly—our abilities to apply maximum force against potential threats.

From this is born an inversion of the Melian Dialogue: At certain levels of engagement, "It is the weak who do what they can, the strong who suffer what they must."[13] Nowhere is this more pronounced than in a collision of interests in which the United States has relatively little at stake, while a weaker adversary sees the issue as life or death.

As long as the stakes of a conflict stay below the level of vital interest to the United States, the weaker power may be able to manipulate the terms of engagement. It is in this area that the initiative lies with the weaker of the two powers. The risk to the weaker power is that either through miscalculation or intent the issue becomes of vital interest to the United States. It has been said that the archetypal asymmetric actor wants to achieve a "Mogadishu, not a Pearl Harbor."[14] If the crossover to U.S. vital interest occurs, the opportunity for effective asymmetric approaches above the tactical level for the weaker party is greatly reduced, and the traditional interpretation of the Melian Dialogue will be reaffirmed.[15] When U.S. national will has been mobilized, the strong will prevail.

Two examples from history demonstrate the two different outcomes. The first illustrates the successful application of an asymmetric approach in an environment where no U.S. vital national interest was at

stake. The second example demonstrates the failure of an asymmetric approach at the strategic level

On 3 October 1993, a task force of Delta Force troops and U.S. Army Rangers attempted to capture key aides to Somali warlord Mohammed Aideed. Although the force used helicopters for insertion and was armed with sophisticated weapons, the operation turned sour. Because of the unanticipated loss of a helicopter, the force became trapped in an urban maze that made it difficult to exploit technological advantages, particularly when the foe was willing to expend prodigious numbers of human lives in densely packed assaults. The confidence of an elite and highly capable unit led it into a situation where it became vulnerable to the Somalia National Alliance (SNA), which had studied U.S. tactics, waited patiently for an opportune window of vulnerability, and sprung an impromptu but lethal counterstroke. American casualties numbered 18 killed and 73 wounded, and hundreds of Somalis died. Often overlooked is the fact that the operation was a tactical success: it accomplished its objective. The effect, though, on decisionmakers in the United States was profound, paralleling that of Tet and Beirut. Certainly the Somali warlords who participated in this fight could not have predicted the enormous effect their encounter would have on U.S. policy in Somalia, but they knew good things would flow from U.S. casualties; the ultimate outcome of the battle was an eventual drawdown of U.S. forces in Somalia.[16] This is an excellent example of how a tactical event, whatever its outcome on the battlefield, can directly influence national strategy, particularly when no U.S. vital interest is at stake.

The second example illustrates the danger of miscalculation. An asymmetric approach that may even be tactically effective can draw the strategic ire of a stronger power by miscalculation. A clear example of this is the Japanese decision in 1941 to initiate hostilities against the United States. The ultimate aim of Japanese strategy was to expand to the south in order to gain unfettered access to oil and other vital natural resources. The American presence in the Philippines was a potent threat on the flank of any such advance, and Japanese strategists concluded that eventually the United States would enter the war against them—it was only a question of when. Given this belief, it seemed reasonable to conduct not only a series of attacks on U.S. forces in the Philippines, but also a spoiling attack on the U.S. Pacific Fleet, forward-based at Pearl Harbor.

Japanese planners calculated that by removing the primary U.S. offensive weapon from play at the very beginning of hostilities, they

would gain breathing room for the establishment of a defense in depth. Even after losses were made good, U.S. forces would have to operate at great distances from home bases when attacking the Japanese Empire. The strategic goal was to induce war weariness in the United States. Viewed in this manner, the Japanese strategy was for a limited war, fought with limited means, and with a limited objective.

Unfortunately for Japan, the attack on Pearl Harbor, while rich with precedent from Japanese military history, had a strategic effect opposite that desired. If Japan had hoped to fight a limited war, Pearl Harbor ensured that the United States would fight a war of unlimited means for what became a virtually unlimited objective: the unconditional surrender of Japan. This well illustrates the open-ended nature of asymmetries: limited tactical successes can ultimately bring massive strategic failure. Pearl Harbor was the key element in the entry of the United States into World War II. The price of miscalculation proved very high for the Japanese.[17]

These two examples highlight the fact that when there is no U.S. vital interest at stake, innovative asymmetric approaches can potentially shape U.S. national will. The danger, as the Japanese learned, is that there can be a fine—and moving—line between the vital and nonvital interests.

Targeting the Will of the Opponent

Asymmetric approaches can achieve powerful effect through manipulation of the psychological element. Aimed directly at the will of the opponent, they can compensate for materiel or other deficiencies. While the method of the approach may be tactical, the psychological effect is sought at the strategic level. This is a key distinguishing feature of asymmetry—the continual focus on strategic effect, enabled by reliance on the psychological component of the approach selected. In functional terms, the target becomes the mind of the opponent, in particular the will of the antagonist. It is a reaffirmation of the Clausewitzian principle that "War is an act of force to compel our enemy to do our will."[18]

Three examples from history illustrate this point. The first, from World War I, is that of Lenin and the sealed train. The Russian Czar had abdicated the Romanov Throne in March 1917, but the Germans still faced a two-front war as the Kerensky government attempted to do its part to keep pressure on the Germans. To the Great German General Staff, the endurance of Russia in the face of staggering defeats was a significant problem. In an attempt to kick-start the squabbling revolutionaries who circled around the Provisional Government in Petrograd and

destabilize the Russian government, the Germans decided to inject a deadly, ruthless, and totally committed communist revolutionary into the body politic of Russia. The revolutionary was Lenin, who, in Winston Churchill's immortal words, was transported "like a plague bacillus from Switzerland into Russia."[19] Lenin, of course, was devoted to the overthrow of all noncommunist governments, so this action shows clearly how desperate the Germans were.

Their bold action paid off in the short term. Lenin energized the communists, and the Bolsheviks seized power from the Provisional Government in the October 1917 revolution and eventually left the war. The Germans achieved their short-term goal: "the greatest possible degree of chaos in Russia."[20] The long-term effect of this injection of ideas was to change the course of world history; ultimately it rebounded upon the Germans in the form of a powerful Soviet Union. There is no clearer case in modern history of the power of an idea used as a weapon. Had the Germans not brought Lenin home from exile, it is unlikely that the Bolsheviks would have seized power as they did, and the course of history would have been different.

A second example of an attempt to operate directly against an opponent's will in the face of serious material and operational mismatches was the Japanese concept for the defense of the home islands in 1945, in the face of an expected Allied invasion. After the fall of Okinawa, Japanese Imperial Headquarters began work on the plans for the defense of the home islands from amphibious attack. They correctly anticipated that the initial Allied attack would fall on Kyushu, southernmost of the home islands and accepted this battle as the decisive one for the defense of the homeland.[21] By this time in the war, Japanese planners had a clear understanding of the overwhelming power of American air support. Their plan of defense, known as *Ketsu-Go*, featured the mobilization of the entire Japanese nation in support of the defense of the homeland. Their intent was to defeat U.S. firepower and maneuver superiority by defending not on the beaches but inland and by avoiding the movement of reserve forces that would become vulnerable to U.S. airpower. By forcing continual close battles and preventing the full application of U.S. firepower, they hoped to cause enough U.S. casualties to weaken civilian morale. The goal was never outright defeat of U.S. forces (except among extremists); instead, it was a rational calculation that, by causing enough casualties in the fight for Kyushu, they might avert the invasion of Honshu.

A third and related example is the adoption of *kamikaze* tactics by the Japanese. This was an asymmetric approach that was never fully solved by the United States Navy. Functionally, *kamikazes* were the antecedents of today's cruise missiles. They were cheap, numerous, and lethal. Off Okinawa and in the Philippines, the U.S. Navy was exposed to the threat. The Japanese inflicted 3,389 fatalities, achieving a ratio of 1.78 Americans killed for each *kamikaze* sortie.[22] This tactic would only become more effective as U.S. forces closed on the Japanese home islands.

The U.S. plan to lessen *kamikaze* attacks was based on attacking Japanese airbases, early warning, effective fighter interception, and point defense. It has been estimated that the Japanese would have been able to generate as many as 7,500 *kamikaze* sorties off Kyushu that might have destroyed as much as a third of the invasion fleet.[23]

These three examples demonstrate the value—and difficulty—of undertaking operations against the national will of an opponent. The example of Lenin and the sealed train has many parallels to information operations today. The examples of the Japanese plan for the defense of their home islands are more conventional illustrations, but all three examples take aim at the will of their foe, rather than its fielded forces.

Attaining Strategic Effect on All Levels of War

Asymmetric approaches have been applied on all levels of war, but the most effective asymmetric approaches seek to attain strategic effect regardless of the level on which they are applied. It follows that there may be a definitional blurring between the level of the action and the level of the effect, and for the asymmetric actor, the goal is to produce effect on the highest possible level.

The strategic level encompasses, in the broadest sense, actions taken to accomplish national-level security and foreign policy objectives. Within the context of asymmetric warfare, these are actions that typically promise the greatest "bang for the buck" for any adversary, since they are designed to influence the basic outcome of a conflict. Actions on the tactical and operational level may yield strategic outcomes, the ideal objective of any asymmetric approach.

A classic example of a favorable strategic outcome deriving from a tactical action is the Beirut Bombing of 1983: The truck-bomb attack on Battalion Landing Team 1/8 in October 1983 ranks as one of the most successful attacks in modern history. It was both tactically brilliant and politically fruitful at the strategic level, since it led to the withdrawal of

U.S. forces from Lebanon in 1984.[24] This episode captures so many of the attributes of a successful asymmetric approach that it could be held up as the "essence of asymmetry." Tactical and strategic surprise were achieved, and the cost to the attacker (probably Syria) was minuscule compared to the blow to American will. This tactical event ultimately had a vastly disproportionate strategic effect, while preventing the United States from responding with overwhelming conventional superiority by obscuring "ownership" of the attack.

The operational level includes actions against theater-level forces and the strategic deployment infrastructure. Of narrower scope than strategic asymmetries, they are regional in focus. A good example of this is the employment of Serbian air defense during Operation *Allied Force* in March-June 1999. During this operation, frequently the Serbian "air defense system simply did not 'come up' to challenge NATO strikes."[25] Most emitters stayed off. This prevented North Atlantic Treat Organization (NATO) air forces from achieving the requisite level of suppression of air defenses, forcing NATO pilots to operate at higher than optimum altitudes when bombing. As General John P. Jumper, Commander U.S. Air Forces Europe, remarked: "We learned from this war that it is a different ball game when SAMs don't come up to fight—everything that we do is based on the bad guy's willingness to engage."[26]

This tactic was, in effect, analogous to Tirpitz' "risk fleet" strategy before World War I, when the very existence of a capability, despite being vastly weaker than its stronger opponent, influenced British planning. In much the same manner, NATO could not afford to ignore the potential resident in the withheld capability. While the Serbs ultimately did not succeed in defeating the NATO air campaign, this approach did significantly reduce its effectiveness. The Serbs were unable to gain strategic effect from this action, and it must be considered a partially effective asymmetric approach.

On the tactical level, asymmetric operations are undertaken against fielded forces, the enabling structures that allow them to operate, and through selection and manipulation of the battlespace. By their very nature, tactical asymmetries often promise the least overall "bang for the buck," even though they may embody remarkable technological or tactical concepts. A clear example of this is Japan's use of the torpedo in World War II. The Imperial Japanese Navy (IJN) placed great emphasis on the torpedo in the years following the Russo-Japanese War, even though torpedoes performed poorly in that war. The IJN always saw itself fighting

from a position of numerical and perhaps big-gun inferiority against potential enemies, and the use of torpedoes at night and in conditions of limited visibility was intended to be a counter.[27] Interestingly, early torpedoes continued to underperform. It wasn't until the eve of World War II, almost four decades after the birth of the torpedo concept in the Japanese Navy, that the IJN finally developed, in the form of the Type 93 oxygen torpedo, the ultimate torpedo of World War II.[28]

This is an excellent example of an organization seeking an innovative way to overcome a perceived deficiency of numbers and firepower by emphasizing a technological counter, yet still applied within an overall symmetric construct of warfighting. It was a very successful asymmetric approach, particularly since it was kept secret from Japan's potential enemies until it had been extensively employed in combat during World War II. Despite significant tactical advantages that accrued from their advanced torpedo technology and doctrine, the Japanese were not able to translate the tactical advantages rendered by the torpedo into strategic results.

The Importance of Effectiveness

Determining effectiveness is critical in evaluating asymmetric approaches. What works and what doesn't work? Effective asymmetric approaches tend to have several common characteristics. From the perspective of the target, they are unexpected actions, and the most effective response may be counterintuitive. The intuitive response may worsen the situation. A good analogy is combined arms warfare; ideally, a force on the receiving end of a combined arms attack will be forced to expose more of its force to another perhaps more damaging form of attack while attempting to compensate for the most visible threat. When executed, effective asymmetric approaches create shock effects within the defender's command system that make it impossible for the defender to attain his original goal,"in practical terms a consequential state of a fighting system which can no longer accomplish its aims . . . which derives from physical and psychological factors alike."[29]

Perhaps most importantly, effective asymmetric operations cause a disproportionate amount of damage to the target for the investment in resources, time, and money by the attacker. Ideally, this effect is felt at the strategic level, regardless of the level at which the operation is carried out.

The importance of effectiveness is illustrated by an asymmetric approach that, while technically elegant and full of promise, failed utterly to gain traction: the Japanese balloon attacks on the United States during

World War II. Beginning in November 1944, the Japanese army conducted a highly sophisticated and sustained countervalue attack on the continental United States by floating large hydrogen gas balloons from launching bases in northern Honshu across the Pacific Ocean in the jet stream. These balloons typically carried several small incendiary and fragmentation bombs. The Japanese intent was to foment panic and instability by setting fire to the huge forest tracts in the Pacific Northwest.

Over 9,300 balloons were launched between November 1944 and early April 1945. Of these, as many as 1,000 reached the continental United States, of which approximately 285 were either recovered or destroyed. Balloons landed as far east as Iowa, and as far south as Texas, although most landings occurred in the Pacific Northwest.

Army Air Force and civil defense planners in the United States rapidly recognized the nature of this threat and clamped a rigid security blackout on all aspects of the balloon attack. This proved vital in denying the Japanese information they could have used to refine their approach and perhaps make their balloons more lethal. On 5 May 1945, six people on a Sunday school outing were killed as they examined a crashed balloon near Bly, Oregon. They were the only casualties caused by this sequence of attacks. There is no evidence of fires started as a result of this effort.[30] This was an ineffective asymmetric approach: the defender was never seriously threatened, and the effective information denial by the United States made it impossible for the Japanese to adjust their approach.

These attacks were unexpected, and for a while they created confusion in the United States (among those who knew about them). On the other hand, they could not provide the disproportionate results that are critical for an effective asymmetric attack, particularly in a situation of total war, when the United States had all the advantages of a fully mobilized economy and the willing assistance of the media in controlling the story.

The Threat-Response Dynamic

Our own actions and strategic choices will drive the nature of the asymmetric threat. As we refine operational practices, potential adversaries will look to find ways to counter. This process of action-reaction is inescapable. Responses by potential adversaries will come from two broad currents: their specific operational and historical-military heritage and outlook, and their reaction to the nature of the perceived threat from the United States.

Cultural Considerations

Nations develop *strategic personalities* over time that can be a useful tool in divining their approach to asymmetric warfare.[31] How has the state traditionally defended itself? Is there a legacy of asymmetric warfare? If the state achieves the capability for weapons of mass destruction, will its outlook be coercive or deterrent oriented? What countries are its potential adversaries, and what is its relationship to the United States? Answers to these questions spring from the culture of the nation and provide revealing clues in looking for potential adversary approaches to asymmetric warfare.

By way of example, the oft-cited German approach to war that proved so effective in 1940–41 had less to do with a search for asymmetric approaches to their potential foes than it did with the affirmation of long-standing core competencies of the Prussian and subsequently the German Army. These included a strong preference for the flanking attack, superior officer training at all levels, and the institutionalization of mission-oriented tactics that encouraged small-unit initiative.[32]

IJN fascination with torpedo tactics, already discussed, is another example. While the use of the torpedo was clearly a response to a perceived tactical disadvantage in quantity and size of big guns, the use of these tactics also harkened back to ancient tendencies in Japanese warfare—the use of small groups of warriors fighting semi-independently against "the heart of the enemy."[33]

Reaction to the Perceived U.S. Threat

This is a particularly difficult challenge for Americans, who often find it hard to see things from the perspective of foreign cultures. We would do well to remember that other nations well understand the ultimate fate of the Melians at the hands of the Athenian Empire. To some, Americans are the embodiment of a modern Athenian Empire. Rumblings from friends in Europe about the United States as a "hyperpower" reflect a growing concern about a unipolar world order.[34] However, the fact that others react to what we do also provides opportunities to influence this eternal circle of action-reaction to our advantage. The choices we make, the emphasis we place on certain programs while de-emphasizing others, can all have a cumulative effect in determining the reactions of others.

A Final Example: The Gulf Tanker War

The recurring themes that have been raised in this chapter can be applied to a recent example. Throughout most of the decade of the 1980s,

Iran and Iraq waged a merciless war that managed to incorporate most of the horrors of 20th century industrial warfare: the indiscriminate use of chemical weapons, "city-busting" attacks with both manned aircraft and SCUD missiles, and naval warfare in the form of attacks on merchant vessels plying the narrow channels of the Persian Gulf.

In February and March 1986, the Iranians appeared to gain the upper hand in the bloody struggle, as their forces finally captured the Fao Peninsula.[35] Growing more desperate, the Iraqis stepped up their attacks on Iranian tankers. This created several problems for the Iranians. It was not possible to reply in kind against Iraq. The Iraqis possessed an insignificant navy, and their oil moved through pipelines into Turkey, or was transshipped from the Gulf States of Kuwait and Saudi Arabia in neutral bottoms. Imports followed the same trail in reverse: to neutral ports in the Gulf (predominantly Kuwait and Saudi Arabia) and then via transshipment to Iraq.[36]

In seeking a way to strike back at the Iraqis, the Iranians were faced with three options: attack the pipelines in Turkey, attack neutral ships carrying war material to Kuwaiti or Saudi ports, or strike tankers carrying Iraqi oil out of the Gulf. All three choices were problematic. The Iranians chose the third option: to attack tankers "in burden" exiting the Gulf from states that were supportive of Iraq. Functionally, this meant attacks on Kuwaiti and Saudi ships, and it formed the core of an asymmetric approach that would be eventually expressed not only strategically—in the choice of the target—but tactically—in the manner of the attack.

Iran had some unique advantages. The Iranian Navy, while greatly weakened from the revolution of 1979, was still the most powerful indigenous navy in the Gulf. Geography also helped. The long coastline of Iran gave ample opportunity to attack the shipping channel that ran the length of the Gulf and the natural chokepoint of the Strait of Hormuz and its approaches in the Gulf of Oman. Because of the bottom contour in the Gulf, the main shipping channel ran in the north, closer to Iran.

Iran had mines, surface-to-surface missiles (SSMs), and a number of small surface combatants with which to execute this strategy. The Iranians also were well acquainted with the potential of mine warfare. In 1973, during a joint exercise with the United States, a senior Iranian officer noted the "vulnerability of the Persian Gulf to guerilla mine warfare."[37] Additionally, the Iranians presumably registered the response of the United States and its allies to the 1984 mining of the Red Sea, during which 19 ships struck mines. The Iranians may have drawn three

conclusions from this. First, it was very difficult to determine who laid the mines. Eventually, strong circumstantial evidence implicated Libya, but there was no "smoking gun." Second, the mines were very effective in reducing traffic in the Red Sea, even though no ships were sunk. This damaged the Egyptian economy, a goal of Libya. Third, the United States took no immediate retaliatory action against Libya. There were, however, contradictory and less reassuring lessons as well. The United States and its allies removed the mines in an international effort, and, eventually, the incident "hardened the Reagan administration's stance toward Libya, leading ultimately to the April 1986 air strikes."[38]

In late 1986, the Iranians began to attack shipping in the Gulf. In 1986, 10 tankers were attacked. In 1987, the number of ships attacked rose to 91. There was nothing the Iraqis could do to stop these attacks, and the Gulf States themselves lacked both the means and the will to take defensive measures. Initially, the Iranian approach seemed to pay dividends, but in December 1986 the Kuwaitis requested information about reflagging their vessels under U.S. colors. Eventually, the United States agreed to reflag a number of Kuwaiti tankers and to provide convoy protection for them and other vessels transiting the Gulf.

The Iranians had little desire to provoke the United States. Despite their inflammatory rhetoric, they pursued a campaign that was designed to hurt Iraq and Iraq's supporters while minimizing the possibility of superpower intervention. The U.S. Navy adopted an operational concept built around "deterrence, intelligence, surveillance, presence, retaliation, and, last, MCM [mine countermeasures]."[39] The initial emphasis was on presence and deterrence. It did not work.

Sometime in the early summer of 1987, the Iranians decided to begin execution of a mine campaign in international waters, although they fastidiously avoided attacking combatant vessels with either their SSMs or small craft. There were dangers for Iran in raising the stakes. Mines, while slightly more difficult to trace to their sponsor, also held the danger of striking a U.S. warship or even a Soviet vessel. On 24 July a reflagged tanker, the *Bridgeton*, struck a mine in international waters while under escort of the U.S. Navy (in fact, *Bridgeton* was the first vessel to transit under protection—hardly an auspicious omen).

The American response was swift. Additional forces were deployed to the Gulf, including MCMs that had not been deployed initially. Over time, the U.S. Navy and its allies were able to establish a strong and credible presence throughout the Gulf. The operational environment was

daunting for U.S. forces: during this period, Iraq continued to aggressively prosecute an antishipping war against Iran, with the tacit approval of the United States. Iraqi attacks on Iran-bound vessels (and, occasionally, by accident on U.S. warships, namely the *Stark* and the *Chandler*) were as frequent as Iranian attacks.[40]

This low level of engagement continued throughout 1987. The Iranians employed mines as their best bet to reduce tanker traffic and other shipments to Iraq. At the same time, Iraq continued to use airpower to strike Iranian vessels. The U.S. Navy and its allies provided escorts for ships en route to the Gulf States—effectively supporting Iraq. In September 1987, the Iranians were caught red-handed laying mines, which largely removed any veil of deniability for them.

Events came to a head in the early spring of 1988, when the Iraqis began a bombardment of Teheran with SCUD missiles, while concurrently retaking the Fao Peninsula, assisted by the use of chemical weapons. On 14 April, Iran's run of good luck with mines ended when the frigate USS *Samuel B. Roberts* hit a mine. The ship was saved by superior seamanship, but the U.S. response was powerful. On 18 April 1988, in Operation *Praying Mantis*, two Iranian oil platforms,a frigate, and several fast attack craft were destroyed. The rules of engagement were extended to enable allied forces to render aid to any friendly or neutral nonbelligerent outside the declared war zone. Because of the geography of the Gulf, Iraqi attacks tended to occur within the declared war zone, while Iranian attacks occurred outside the zone.[41]

The turn of fortunes in the ground war, coupled with the disastrous events at sea, forced Iran to reevaluate its policies. It had attempted to apply an asymmetric approach to the task of hurting Iraq's economy, while rheostatically controlling the likelihood of an encounter with the U.S. Navy. The principal weapon was mine warfare. While Iran did some limited damage to Iraq's war economy, ultimately the war of the tankers was a failure for Iran. It exemplifies the open-ended and unpredictable nature of asymmetric approaches. The instrument proved too blunt, and eventually a U.S. warship was struck. Iran was not prepared to risk war with the United States, even when the USS *Vincennes* mistakenly shot down Iran Air flight 655 on 3 July 1988, with heavy loss of life. Surprisingly, the shootdown of the flight may have provided the catalyst to end the Iran-Iraq war. Iran was too exhausted to continue and, in mid-July, accepted the terms of a UN cease-fire.[42]

What can this case study teach us? First, the Iranians understood that they had some advantages in confronting the United States only so long as they were able to maintain an asymmetry of interest. They consciously made decisions in this light, refraining from taking escalatory actions that they judged would be viewed as inflammatory by the United States. Ultimately, they were unable to prosecute this strategy, but the failure lay in execution rather than the concept itself, which sought to minimize the possibility of a conflict with the United States.

Second, the Iranian use of mines and other forms of unconventional naval warfare sought disproportionate effect at low risk and cost. They were able to achieve this at times, but ultimately they were unable to execute this component of their strategy. This reflects an Iranian misreading of the effects of mine warfare and access denial strategies upon the United States, since these were the issues that provoked an enlarged United States presence in the Gulf—exactly the opposite of what the Iranians desired.

It is important to note that, in the final analysis, the Iranians were the losers in this struggle, and their defeat was a strategic disaster of the first magnitude for them. The tactics and technologies they applied were unable to carry the load of a dual strategy that sought to strike at the Iraqis while minimizing United States (and its allies) presence in the Gulf.

This is a particularly important case study for yet another reason: it may foreshadow future adversary asymmetric approaches, both in terms of strategy and technology. The Iranians chose a relatively low-risk and deniable approach, and they implemented it with what they hoped were cheap, nonattributable tactics using a relatively low technology weapon—mines. The overall strategy had some merit, and its failure does not mean that we will not see some variant of it again. Finally, it's worth noting that a number of escalatory options against the United States and its allies were never executed by the Iranians. Their attempt to manage the conflict with the United States and its allies in the Gulf while fighting a total war with Iraq demonstrates considerable strategic sophistication. It is likely that dual-track approaches of this nature will recur.

Conclusions

This chapter has sought to define asymmetry by examining the current definitions, and then to refine existing thinking by explicitly proposing the concept of disproportionate effect as the desired outcome

of an asymmetric approach. Five recurring features of asymmetry have been identified and are useful in understanding asymmetry:

- Disparity of interest is a key factor in assessing an adversary's incentive to adopt asymmetric approaches.
- The will of the opponent is the ultimate target, and understanding this is fundamental to understanding asymmetric warfare.
- Asymmetric approaches operate on all three levels of war, but seek strategic effect.
- Effectiveness is important in evaluating asymmetric approaches (they don't always work).
- A dynamic process of threat and response is an inescapable factor in any analysis of asymmetry.

The examples that attend each of these themes demonstrate that asymmetric approaches are not new to the strategic landscape. They also demonstrate that innovative and exotic thinking can produce dramatic benefits for the weaker power in a confrontation. What gives immediacy to the study of asymmetry is the realization that new weapons and capabilities are creating new vulnerabilities. Many of these new weapons have characteristics that are ideal for use in an asymmetric approach.

The idea of disproportionate effect is particularly compelling as a jumping-off point for chapter two. In evaluating the historical development of asymmetric approaches, the most ominous conclusion is that the potential destructiveness of these asymmetric approaches has increased dramatically in the latter half of the 20th century. The confluence of nuclear weapons, chemical weapons, and biological weapons with actors who are searching for cheap and innovative ways to address strategic imbalances makes the possibility of catastrophic outcomes far greater than at any time in the past.

Chapter Two

A Typology of Asymmetry: What, Who, and When?

Building upon the recurring themes established in chapter one, this chapter will attempt to organize and draw some useful conclusions about the range of potential asymmetric threats that we could face through the year 2010, using the framework of *what*, *who*, and *when*. First, *what* are the general types of potential asymmetric approaches that we could reasonably expect to see employed? After these have been established, the *who* will be considered, from a conceptual basis. Last, the question of *when* will be discussed. Timing is important in asymmetry, and different approaches are more likely to be employed at different times in a crisis. The chapter will end with a discussion of general conclusions that can be drawn from this analysis.

The What: The Range of Potential Asymmetric Threats

This section identifies a typology of six potential asymmetric threats: nuclear, chemical, biological, information operations, operational concepts, and terrorism. Each potential threat will be discussed and assessed within each of the three levels of war, with a focus within the level of war to which its effects could reasonably be expected to predominate. The most likely concepts for employment of these threats will be discussed and analyzed. Why these six categories of threats? They are logical descendants of asymmetric approaches used throughout history—they all promise disproportionate effect, and all have the potential to migrate effects upward to the strategic level. There are key differences from the past, however: the greatest change at the beginning of the 21st century is the dramatically increasing effectiveness of technology and its ability to conjure global effect from local events. The most dramatic and potentially lethal threats are those associated with the ugly triad of weapons of mass

destruction (WMD). The newest threats arise from the explosion of information technology.

In this six-part typology, the WMD elements of *nuclear*, *chemical*, and *biological* have become the "usual suspects" when discussing asymmetric threats. They are dangerous, to be sure, but there are alternatives open to the asymmetric actor. *Information operations* involve the manipulation, both offensively and defensively, of data of all types. The term can also refer to the denial of information-intensive operations fundamental the American military's operational doctrine. *Operational concepts* refer to the broad application of "low technology" and "no technology" approaches to asymmetry, as well as to the innovative application of legacy systems and tactics. *Terrorism* refers to the actions of nonstate actors, both internal and external, who may apply approaches from the other elements of asymmetry.

Nuclear Weapons

The ultimate expression of power in the world today is the possession of nuclear weapons. Owning nuclear weapons allows a state or nonstate actor to have a seat at the "high stakes" table. This idea has been reinforced by such recent events as the Gulf War and NATO operations over Kosovo. The former Indian Army Chief of Staff, General K. Sundarji, is reputed to have said that a principal lesson of the Gulf War is that, if a state intends to fight the United States, it should avoid doing so until and unless it possesses nuclear weapons.[43]

Despite the frightening specter of a dispersion of nuclear materials from the former Soviet Union's massive stockpile, nuclear weapons essentially remain the province of states.[44] Nonstate actors do not possess the combination of skill, focus, and organizational ability to build them (although they could steal or buy them). Nuclear weapons are technically demanding to build, even for moderately industrialized states, and creation of a first-generation atomic capability is a long way from effective weaponization, which implies miniaturization, hardening, effective targeting, command and control, and means of delivery. It is important to note, though, that nuclear weapons can be employed without miniaturization, although the problem of delivery becomes more complex and demanding.

For these reasons, for the next decade or even longer, the number of states that possess indigenously developed, reliably deliverable nuclear weapons will be very small: the United States, Russia, France, England, China, and Israel.[45] Of these, Russia, France, China, and England have the unambiguous capability to deliver a "conventional" (i.e., ballistic missile)

attack against the continental United States. The second circle of states that possess self-developed nuclear weapons that may be—and certainly eventually will be—weaponized is composed of Pakistan and India.

Other states could join this club by obtaining weapons or fissile material from external sources, and the countries and sources are obvious: Iraq, North Korea, and Iran. All may be attempting to obtain either complete weapons or near-assembly-ready components from former Soviet stocks. It is possible that these states may be closer than we know.

Tactical Employment

On the tactical level, a nuclear weapon could be employed directly against maneuver or support forces in the field. The method of delivery could range from short-range ballistic missile or tactical aircraft delivery to mining or other covert means. In this context, the asymmetry of approach is principally derived from the deterring effect that adversary possession of such a weapon would have on U.S. responses to crises. Actual state-sponsored use of a nuclear weapon against forces in the field is the least effective method of employment of a nuclear weapon—in fact, in many ways it is no more than the ultimate symmetric response.

Adversaries will be hesitant to employ nuclear weapons on the tactical level for several reasons: first, unless the attack is a complete strategic surprise, tactical maneuver forces can disperse rapidly, making it hard to achieve military effect commensurate with political cost. Second, it will be very easy to trace ownership of the attack, particularly if it is delivered by conventional means. Third, use of nuclear weapons against U.S. forces will almost certainly invite a staggering response that might not stop short of the imposition of unconditional surrender. Last, adversaries will not have many nuclear weapons, and targeting fielded forces is surely the least cost-effective method of employment.

If an adversary decides to employ nuclear weapons in this manner, conventional means—ballistic missile, tactical aircraft—are the methods that have the least chance of success, while leaving a clear trail back to the attacker. Missiles and aircraft can be intercepted, and the attacker may not have the technological confidence to hazard such a critical attack with such an unsure means of delivery. The greatest chance of success against fielded maneuver forces may be the employment of either covert means of insertion by special operations forces (SOF) or terrorist operatives, or by the use of nuclear mines. The use of nuclear mines is appealing, particularly in a defensive situation in which the adversary is giving up ground to a U.S. advance. This would permit hardening and the

use of various concealment measures that might make the device harder to discover before detonation.

For these reasons, states that have nuclear weapons will be loath to employ them directly against U.S. forces. They may be more likely to employ them against allied or coalition forces, who generally will be less prepared to deal with nuclear attack. They may also be more likely to attempt to target fixed combat support activities, such as airbases.[46] Another possibility is the targeting of U.S. warships, particularly modern cultural icons like aircraft carriers. The lure of this is complicated by the formidable difficulty of delivering a weapon close enough to damage a carrier.

Nuclear weapons will have the most potential utility in the early stages of a major theater war, when they can threaten or deter U.S. deployment into theater. They will be of less utility after U.S. forces close and the theater matures, but they will again become a significant factor in the end-state of a major theater war, particularly if the adversary sees the possibility of cataclysmic defeat. In this case, the temptation will be strong to use any and all means in a spasmodic response to either change the tide of battle or simply inflict revenge on the United States or its allies.

The use of nuclear weapons against U.S. forces on the tactical level is unlikely at the hands of a rational state actor. The tactical employment of nuclear weapons against forces in the field isn't really a practical asymmetric approach. If executed, it would tend to create a case of "vital national interest" for the United States, where perhaps there wasn't one before. The concept of disproportionality would then be turned upon its head, and high risks would be accrued by the actor with very little gain. The threat of use is more problematic, although threats against fielded forces also carry many of the risks of a deterring strategy while reaping few of the advantages.

Operational Employment

Nuclear weapons can be employed against the deployment and theater support infrastructure in order to deter, slow, or even halt the deployment of forces into an area of responsibility (AOR). Attacks against fixed targets will obviously be easier to plan and execute than attacks against forces in the field. The advantage of employment against fixed, rear area targets is that instead of targeting the most-prepared forces (usually tactical maneuver forces that possess organic mobility), targets can be selected from nonmobile forces that will have less self-protection and little ability to move.

The same delivery considerations apply as on the tactical level. Ballistic missiles, manned aircraft, or SOF can all be employed to deliver nuclear weapons against airfields, ports, command posts, logistic areas, or even humanitarian lodgments—all with a greater degree of confidence than at the tactical level, because these targets are, by and large, fixed and nonmobile. To borrow a term from Cold War strategic nuclear doctrine, at the operational level, asymmetric targets increasingly become countervalue, instead of counterforce.

It follows that, for a state actor, the greatest opportunity to employ, or to threaten to employ nuclear weapons, will be in the early stages of a conflict. The intent will be to initially deter and complicate U.S. force deployment considerations, and potentially to destroy critical deployment infrastructure in order to actually prevent physical deployment. If employed early enough, critical aerial ports of debarkation (APODs) and surface ports of debarkation (SPODs) might be destroyed or degraded before U.S. forces even arrive, creating an ambiguous situation for the National Command Authorities (NCA). It seems clear that if nuclear weapons are employed against U.S. forces, the response will be overwhelming and direct; but what if they are employed against an ally, and few, if any, U.S. forces feel the results?

The use or even threat of this may well dampen the enthusiasm of potential U.S. allies for participation in a coalition structure. It may well be that the direct threat of nuclear employment against an ally or potential ally very early in a crisis will have the effect of dissuading that nation from participating with the United States in a coalition. This threat of operational-level employment of nuclear weapons against U.S. regional allies or partners has the greatest promise of strategic effect migrating upward from an operational act for a regional actor. In terms of actual use, targeting both political and military supporting structures instead of fielded forces promises far greater return than direct tactical employment.

Strategic Employment

By definition, this is the threat or the use of a nuclear weapon against the U.S. homeland. In this case, strategic effect is sought by direct strategic attack. In considering the utility of strategic nuclear attack, it seems clear that, for a regional power or rogue state, the greatest asymmetric utility for these weapons is in their deterring effect. A demonstrated, credible ability to strike the U.S. homeland will have a sobering effect on U.S. decisionmakers as they consider bombing a regional adversary's capital, or even deploying forces in the face of threats or warnings

when U.S. vital national interests are not at stake. It is even possible that the possession of nuclear weapons, and the demonstrated (or even suspected) capability to deliver them against the American homeland will have the effect of compressing the box within the quadrant marked "U.S. interest is vital" in the asymmetric opportunity table in chapter one. It may require unambiguous vital interest indeed for an American president to attack a state that has the capability to execute a countervalue attack on the United States.

There is another side to this argument, though, and that is when an asymmetric actor crosses the nuclear Rubicon from deterrence and coercion to actual use. It is difficult to conceive of a rational actor electing to employ nuclear weapons against the United States in a direct strategic attack. To do so would invite annihilation. Given this, though, the deterring effect of a U.S. response will certainly erode in a war in which the regional actor sees events going badly against it. If it looks as though the United States and its allies plan to either bomb a country to submission or occupy its capital, then there is little to lose, and in a *götterdämmerung* scenario, the possibility of actual strategic employment becomes increasingly likely.

Few states have the capability to deliver such a weapon by conventional means (aircraft or missile), and the robust nature of the U.S. strategic warning system is such that even if a successful attack were generated, clear and unambiguous evidence of the source would probably be readily available. Delivery by covert means is a more difficult subject. A nuclear weapon could be brought into this country by any one of a hundred methods, and could be positioned against a countervalue target by competent SOF. If the United States were engaged in a confrontation at the time, the motive and attacker would be clear. Even without strategic forensic evidence, the linkage would probably be enough to allow a massive response. The issue becomes more clouded when dealing with a bolt-from-the-blue attack at a time when identification of the attacker would be difficult to establish. Perhaps even a third party would initiate such an attack with a view to provoking the United States to retaliate against the presumptive guilty party—a false flag tactic.

Targets in the U.S. homeland would almost certainly be countervalue. It is unlikely that any potential adversary would be able to infiltrate or launch enough weapons to achieve significant strategic-level military results from such an attack.[47] Given the tremendous political considerations of a nuclear attack on U.S. soil against any target, the logic would tend to drive a potential attacker to seek the most lucrative and shocking

option. Major urban areas, such as Washington, New York, Los Angeles, or Chicago, would probably lead the list of alternatives. They are also the easiest to target because of their size.

In an extended major theater war, aggressive U.S. efforts to destroy or neutralize a foe's nuclear delivery structure may result in another response from the heart of the Cold War—a "use 'em or lose 'em" reflex. In this case, an opponent cannot stand by and see its strategic trump card taken away. This does not imply that U.S. forces should not attempt to do this, only that we must be prepared for an adversary to use its weapons if we engage in aggressive WMD reduction during a regime-threatening war.

The *threat* of using nuclear weapons directly against the U.S. homeland is a powerful asymmetric measure. It achieves clear strategic effect and operates directly against the will of the United States. Such an approach might very well tend to make the United States ask hard questions about just where its vital national interests lie. Many of these asymmetric advantages could easily be lost, however, if a threat were actually carried out. A nuclear attack would provoke a powerful and unrelenting response from the United States. There is a fine line between the positive disproportionate strategic effect achievable by the possession of nuclear weapons, and the potentially disastrous consequences of actual use against the United States.

The last consideration is the use of nuclear weapons by nonstate actors against the United States. It is the least likely alternative because of the difficulty of procuring, infiltrating, and emplacing the weapon. It is, however, a possibility, and may ultimately prove the most troubling of all the strategic nuclear threats. Such an attack could be just as damaging as anything launched by a state actor, but it would be difficult to establish responsibility.

Conclusions About Nuclear Weapons

Martin van Creveld has written that the development of the atomic bomb and the concentration camp are together the most significant expressions of the power of the state in this century.[48] The threat of use of nuclear weapons has the greatest effect on the strategic level, although threats on both the operational and tactical levels will create similar disproportionate benefits. In terms of actual employment, use against regional supporting infrastructures is probably the most effective. This underlines the idea that it will never be a good idea to use nuclear weapons directly against U.S. forces or the U.S. homeland.

For these reasons, it may be that nuclear weapons will pose their greatest threat when used in a technically nonlethal role—as the generators of high-altitude electromagnetic pulse (HEMP) that will threaten our information systems. For that reason, the threat of HEMP attack will be dealt with in the discussion of information operations.

Chemical Weapons

Of the three elements of WMD, chemical weapons are generally considered to be the least damaging. On the other hand, they are also the easiest to procure, and, if history is any guide, less stigma is associated with their use. They have been used extensively by Iraq against not only Iran, but the Kurds.[49] A large number of states possess some form of chemical weapons. (As of December 1997, 106 states had ratified the Chemical Weapons Convention [CWC] of 1993.[50] China, Cuba, Egypt, Iran, Iraq, Israel, Libya, Myanmar, North Korea, Pakistan, Syria, Taiwan, Yemen, and the former Yugoslavia are all suspected of maintaining some form of chemical weapons stocks.[51])

Tactical Employment

As with nuclear weapons, the use of chemical weapons on the tactical level against U.S. maneuver forces—the most-ready part of the U.S. force structure—is cost-ineffective. Some of the delivery complications that apply to nuclear weapons are also operative here, although the use of shorter-range artillery and tactical rocket delivery may partially ameliorate this. Chemical weapons will be more effective when used in conjunction with imaginative and potentially asymmetric operational concepts, such as defense in depth in complex terrain. The application of chemical weapons against refugee or other noncombatant populations could be an attractive option that could stress the capabilities of U.S. forces to care for both themselves and a large pool of suffering noncombatants and dramatically cloud the picture of the battlefield.

U.S. forces are generally well prepared to fight and win in a chemical environment, both as a legacy of decades of preparation to fight the Soviets and as a function of a renaissance of tactical chemical awareness in the past five years. Even so, the use of chemical weapons on the tactical battlefield will tend to slow the tempo as units are forced to don protective overgarments and conduct chemical reconnaissance and frequent decontamination. Slowing the tempo of operations will be a key component of any attempt to counter U.S. dominance.

Allied forces may be less well prepared, and this is the critical weakness that may be exploitable through asymmetric approaches on the tactical level. Attacks against allied forces will require the United States to provide support for less capable forces, stretching thin our capability to provide adequate chemical defense coverage for our own forces. At the same time, the use of chemicals against allies instead of the United States in a coalition may avoid a massive U.S. response. At a minimum, it will create an element of ambiguity when weighing responses.

The bottom line is this: using chemical weapons against tactical U.S. maneuver forces will not change the basic dynamic of a campaign. The use of chemical weapons will slow the pace of fighting, but it will not change the formula of victory. Since this is the application of a weapon of limited effectiveness against a strong and prepared opponent, it is hard to consider chemical employment against U.S. forces in the field as a potentially effective asymmetric approach. Used in this manner, it really isn't an asymmetric approach. It doesn't achieve disproportionate effect, and there is little possibility for upward migration of effect. It may also spark a massive U.S. response.

On the other hand, employment against allied units or a civilian population remaining on the battlefield may prove to be far more effective. Such an approach may bring an adversary huge political dividends as well, if the United States is unable to rapidly correct potential deficits in allied chemical defense training and equipment, and provide succor to threatened civilians. This approach does promise disproportionate effect, and may well be able to achieve significant strategic effect through an aggressive information operation.

Operational Employment

Many of the considerations regarding nuclear weapons apply also to the use of chemical weapons on this level. The most likely targets will be the deployment infrastructure that allows U.S. forces to enter a theater, command and control facilities, and the combat support and combat service support infrastructure that support the operations of U.S. and allied air forces. Another potential target will be the host nation population in the theater service area, with the intent of stressing host nation, allied, and U.S. medical support systems as well as political unity.

There are a number of potential delivery options, ranging from ballistic and cruise missile to SOF, aircraft, and terrorists. The most cost-effective option may be cruise or ballistic missiles. This choice of delivery systems will be dictated by the relatively inefficient size-to-lethality ratio

of chemical weapons, as well as the probable difficulty of manned aircraft penetrating deep into a theater area (although this may be more attractive in an immature theater, before a comprehensive U.S. integrated air defense system is in place). Special operations forces can be used to employ chemicals on the operational level, but the size of the mixture needed to be effective, as well as the difficulty of efficient dispersal, will tend to reduce the effectiveness of this approach. As with nuclear weapons on the operational level, the threat of employment of these weapons can be effective in splitting alliance partners away from the United States in the early stages of a regional crisis.

Strategic Employment

Chemical weapons can play a role in strategic attack, which, as with nuclear weapons, means an attack on the U.S. homeland. While they are less lethal than biological agents and not as destructive as nuclear weapons, they are inherently more stable (an important consideration when dealing with less well-trained operatives) and can still be very effective, particularly when employed against indoor and point targets.

Chemical weapons do not have the shock and horror cachet of biological or nuclear ones, but that is a relative consideration—a few pounds of VX or SARIN deposited into a busy subway station in New York or Washington would have a tremendous psychological effect. The example of Aum Shinriko's attack in the Tokyo subway, incompetently executed and with diluted SARIN, is cautionary.[52] Perhaps the greatest distinction between chemical weapons (and biological weapons) and nuclear weapons is that it may prove more difficult to trace the origin of a strategic chemical or biological attack. For this reason, the threshold of employment may be lower than with nuclear weapons.

Conclusions About Chemical Weapons

Chemical weapons are the least potent of the WMD triad. They do not have the open-ended potential for disaster that haunts both nuclear and biological weapons. They are easier to produce than nuclear weapons but require a larger and more visible infrastructure than that required for biological agents.[53] They have a track record of use throughout this century, which probably means that we will continue to see them employed.

Across the spectrum, chemical weapons offer the most asymmetric effect when employed as threats against regional allies. A regional aggressor can normally expect to be able to threaten the homeland of adjacent states with these weapons. Employment in this manner promises

strategic effect at a relatively small cost. Even if an actor is forced to carry through on its threats to actually employ these weapons, scrupulous attempts to avoid U.S. forces may make it very difficult for the United States to respond forcefully, while possibly crumbling a regional alliance.

Biological Weapons

An interesting historical parallel may be developing. In the first decade of the 20th century, the all-big-gun *Dreadnought* battleship became emblematic of national power. These ships were built (or ordered) not only by leading powers like England, Germany, and the United States, but also by lesser powers like Chile, Greece, and Turkey, which had no obvious compelling reason for their use. Even as the numbers of these ships grew, though, the hidden dynamics of war at sea changed their utility, and they were supplanted by the aircraft carrier as the ultimate weapon. Few of these magnificent weapons were ever employed. In much the same way today, even as lesser states pursue the nuclear totem, it may well be that in the 21st century nuclear weapons will be relegated to secondary status behind biological weapons. The latter are cheaper than nuclear weapons, easy to move or hide from prying inspectors, and, most importantly, profoundly lethal. They can be employed in a manner that might make it hard to trace sponsorship of an attack.

A key distinction needs to be established at the beginning of any discussion of biological warfare. While there are many different types of biological agents, they may be catagorized as either contagious or noncontagious agents. The former can be passed from one human host to another, either directly or indirectly. The latter cannot be passed in this manner. This has no bearing on lethality or infectiousness; noncontagious agents like anthrax could have lethality rates in excess of 80 percent in an unprotected population, which indicates a high degree of infectious reliability.[54] A contagious agent such as plague has the potential to ultimately reach a much larger proportion of the targeted population. Minimal contagiousness generally has been a desired characteristic of biological weapons, although there are contrary views.[55] In World War II, the Japanese developed plague, a highly contagious agent that also had high lethality and infectious reliability, and planned to employ it against the United States.[56]

The Biological Weapons Convention (BWC) of 1972 outlaws the possession of such capabilities.[57] Despite this, there is compelling evidence that the Soviet Union and its successors continued to work on an offensive biological warfare program "at least until 1992."[58] Other states,

including China, Iran, Israel, Libya, North Korea, Syria, and Taiwan, are believed to have produced operational quantities of biological weapons.[59] Iraq is believed to possess a capability as well, despite the best efforts of United Nations inspectors in the wake of the Gulf War.[60]

Tactical Employment

Biological weapons, like all WMD, are less effective on the tactical level, for many of the same reasons that pertain to chemical weapons. Biological agents are even more volatile and susceptible to biodegradation and corruption than chemical agents. They are also more difficult to disperse over a wide area. The most likely dispersal options for an opponent would include rocket artillery, artillery, aircraft, and SOF. The principal problems would be devising methods to protect the biological cargo during transit to the target and ensuring adequate area coverage in an open environment. Weather and time of day are of fundamental importance in selecting attack profiles.

The target of a tactical biological weapon attack may well be inoculated against the most common agents. In short, on the tactical level, the use of biological weapons is another case of an attack against the strongest part of the defense, something that is counter to asymmetric warfare. The same considerations that apply to the tactical use of chemical weapons apply here—this isn't an asymmetric approach, although the use of biological weapons against a civilian population within a battlespace could create problems even more significant than those caused by chemical weapons. The medical stresses in particular could prove far more complex and long term.

Operational Employment

The use of biological weapons against theater-level targets offers the most lucrative and cost-effective employment option of all forms of WMD use. Biological weapons enjoy the same deterring effect as chemical weapons on the operational level, but they can be far more potent in effect. The threat of anthrax, tularemia, or Venezuelan Equine Encephalitis (VEE) against a theater APOD or SPOD that depends upon host nation support could have a crippling effect on the flow of U.S. forces into theater. They are more attractive than nuclear weapons because it is more difficult to trace sponsorship of an attack.

Many airlines, including those mobilized in support of U.S. deployments (the Civil Reserve Air Fleet, or CRAF), may not fly into areas with reported biological weapons attacks.[61] Without these critical enablers,

it may not be possible to complete the deployment of U.S. forces into a theater of operations. The use of anthrax (for example) in even small quantities might cause heavy casualties and tie up medical and other infrastructure; even the hint of its use, coupled with an aggressive information warfare campaign, might turn our strategic deployment structure on its head. Additionally, theater infrastructure, such as command posts, logistics nodes, and other key elements of the combat service support backbone, is vulnerable to these attacks.

It might be very difficult to establish clear culpability in the case of the employment of a biological weapon. Unlike the nuclear or chemical weapon that is delivered via a cruise or ballistic missile, biological agents, by virtue of their extremely favorable weight and cube to lethality ratio, lend themselves to covert application by SOF. While we are certainly not defenseless against these threats, clear evidence to trace ownership may not be available.

Biological weapons offer many of the same coercing virtues of nuclear weapons within a regional environment. The principal advantage of biological weapons will be the potential for employment without clear responsibility. If introduced by SOF or terrorists, it might be very difficult to link a regional actor to a specific attack—however strong the motive and our suspicions. For this reason, they represent ideal asymmetric approaches. While the attack will be operational, the effect will be strategic.

Strategic Employment

A host of recent movies and books, such as *The Cobra Event* by Richard Preston, have highlighted this threat, and it joins nuclear attack at the most-dangerous end of the scale. When considered for its potential coercing or deterrent value against the United States, this threat enjoys every advantage of the strategic nuclear threat, but it can be delivered in a more covert manner. For this reason, the firewall between deterrence and use may not be as strong as in the nuclear case. There may be a greater likelihood of employment. As outlined in the operational and tactical discussions above, biological weapons are much easier to deliver than nuclear weapons, and, depending upon the agent used, the attack might not even be recognized until well after the fact. Biological attack also is more deniable than nuclear attack.

Biological weapons become even more of a threat when considering nonstate actors, particularly terrorists, although the likelihood of use decreases. While not minimizing the threat, it is useful to consider that no "mainstream" terrorist organization has ever elected to pursue

this method of attack.[62] On the other hand, increasingly radical terrorist organizations, including those with millenarian views, may not have this restraint. It is reassuring that the organizational skills, scientific knowledge, and cool heads (and hands) required for the conceptualization and delivery of a biological weapons attack are not normally associated with radical terrorist groups.

Conclusions About Biological Weapons

Nuclear and biological weapons share an unfortunate commonality: they can end the world as we know it. Biological weapons are easier to produce and easier to hide than either nuclear or chemical weapons.[63] The method of attack can be circumspect and difficult to trace. When employed to deter, they can achieve strategic effect, and,like nuclear weapons, cause the United States to compress the "vital national interest" box. If a bluff is called, they can offer the advantage of forensic ambiguity. For these reasons, in the short to mid term, biological weapons will increasingly become the tool of choice for both state and nonstate actors contemplating asymmetric approaches. The likelihood of actual employment is higher in a regional theater of operations than directly against the continental United States. At the same time, the implicit threat of use as a deterring or coercive tactic against the continental United States will only rise.

Information Operations

The modern U.S. military's concept of fighting is built upon the rapid, efficient exchange of vast amounts of information.[64] In this, it mirrors the cultural and business explosion of information exchange unleashed in the last 20 years by the power of the personal computer and the worldwide web. This global system supports not only the financial well-being of the United States, but also the operation of an increasing proportion of the physical infrastructure necessary for day-to-day life in the United States, from air traffic control to hydroelectric plant management. Allied with this is the growth of a global culture that fosters the rapid exchange of information on a bewildering variety of subjects. This is the environment, ripe with both promise and danger, for information operations.[65]

Tactical Employment

It is difficult to compete with the United States technologically on the tactical level. Tactical combat information systems are generally well protected and resistant to direct attack. The best asymmetric approaches

will probably be passive: camouflage, clutter, and concealment—techniques that will make it hard for U.S. intelligence-gathering systems to gain a clear picture of the battlespace. This could be coupled with aggressive deception operations and a psychological warfare campaign that seeks to magnify U.S. missteps. This means taking advantage of the fact that in a world of near-instantaneous global communications, a tactical event can have immediate strategic effect. The bombing of the al Firdos command and control bunker in downtown Baghdad during the Gulf War while it contained civilians, and the mistaken bombing of an Albanian refugee convoy during *Allied Force,* are but two examples of U.S. tactical actions with adverse implications that were magnified immensely by adversarial manipulation of information—and by our own clumsiness in responding.[66] Denial or degradation of our superior battlefield vision, coupled with relentless attempts to gain strategic effect from U.S. tactical missteps, will characterize adversary tactical information operations.

Operational Employment

On the operational level, it will become easier to enter and conduct computer network attack (CNA) against the family of systems, both classified and unclassified, that support the U.S. deployment infrastructure. This is because an increasing percentage of information traffic will be carried on systems external to the Department of Defense (DOD).Our allies and coalition partners will be at least as vulnerable. Even the well protected U.S. defense internet systems are dependent to some degree upon unclassified routing and vulnerable public domain structures as they go through what has been called the "last mile" between the DOD maintained NIPRNET (nonclassified internet protocol router network) and the end user.[67]

At the same time, adversaries will target regional allies and any coalition structure with psychological operations and propaganda. When conducted in conjunction with the threat or actual use of other asymmetric approaches (i.e., WMD), a powerful synergy can be obtained, linking information operations with events on the ground, whether real or imagined. Charles Dunlap, writing in *How We Lost the High Tech War of 2007,* outlines an extreme but thought-provoking scenario: a regional opponent might elect to employ nuclear weapons against his own population, blaming the United States for the attack.

The management of publicly released information will remain a core competency for any crisis. What people see, read, and hear both in the United States and abroad will ultimately shape their perceptions of

the rightness or wrongness of our cause. While this effort will feature a number of high technology aids, the fundamentals remain the same as they were during World War II: "This was total war, and total war required the calculated circulation of facts, which were a weapon more deadly than bullets and bombs."[68]

Strategic Employment

A potential cyber attack against the U.S. homeland has probably received more recent media attention than any other form of asymmetric warfare. As a society, the United States is both relatively and absolutely more dependent upon computer systems for activities ranging from personal banking to management of highways than any other nation in the world. Some of these systems are protected, most are not, but virtually all are interlinked to some degree that increases their vulnerability.[69] Our ability to identify and defend against these potential attacks is fragmented—to some extent simply because of the breathtaking scope of the threat. It may prove very hard to identify attackers, and the line between criminal activity and state-sponsored attack will be blurred.

This will remain one of the most potentially effective domains for an asymmetric opponent. An attacker will be able to maintain a high degree of deniability, and the potential for damage is unlimited. The nearest analogy is to strategic biological warfare, where an open-ended threat is coupled with a target-rich environment that is only partially protected.

HEMP—The Underestimated Threat

Perhaps the most dangerous and misunderstood form of information warfare attack is the high-altitude electromagnetic pulse (HEMP) threat: a combination of nuclear weapons and information warfare that can challenge the very heart of our operational doctrine and national stability. For this reason, it will be dealt with under this heading, although it has obvious application at other levels of war.

HEMP is a principal byproduct of the explosion of a nuclear weapon detonated above the earth's atmosphere, typically above 30 kilometers. The environments produced by a nuclear explosion can be considered direct (e.g., mechanical) and indirect (e.g., electrical). For an explosion at or near ground level, the direct environments are the most obvious, and are the results of the conversion of the bomb's potential energy into thermal and kinetic forms, resulting in fire and blast damage.[70] Thus, the obvious physical environments of a nuclear explosion—the fireball, blast, light, and heat—are direct environments. One indirect effect of a nuclear

explosion is the electromagnetic pulse that results from the conversion in the earth's atmosphere of gamma-ray energy to radio frequency energy that propagates toward the earth's surface.[71]

The higher the altitude of the explosion, the less the direct effects (blast) of the weapon, and the greater the indirect effects (HEMP) will be; an exoatmospheric burst would be optimum.A burst at an altitude of 300 kilometers, for example, would have several important impacts: first, a greater altitude would expand the line-of-sight coverage of the burst (and HEMP is a line-of-sight effect), but would also reduce the HEMP fields over what could be produced at lower altitudes (each weapon has an optimum burst height to produce the largest HEMP fields). At 300 kilometers, a burst centered over central Nebraska could generate HEMP environments over 90 percent of the continental United States.

Space systems are uniquely vulnerable to nuclear radiation outputs and dispersed EMP, which is a derivative environment produced by HEMP, as well as exposure to delayed radiation effects, resulting from potential enhancements to the Van Allen belt following high altitude explosions above 40 to 50 kilometers (a lower burst height will not have as much effect).[72] A particularly ominous aspect of the danger to space systems is the fact that an exoatmospheric explosion anywhere over the surface of the earth could affect satellites. A nation seeking to threaten satellite systems might choose to detonate the warhead over its own territory, for example, with the goal of "pumping" the Van Allen belt. It has been estimated that in 1995 there were over 40 declared satellites on low earth orbit (LEO) performing "a variety of military, commercial, and scientific missions that would be threatened."[73] Ongoing launch programs since then have added large numbers of Teledesic, Orbcomm, and Globalstar communications satellites. All of these systems are potentially vulnerable to trapped radiation belts and dispersed EMP from high-altitude bursts. While it is likely that not all satellites would "go down" as the result of "single event effects," the increase in the total ionizing radiation accumulation at satellite altitudes will dramatically shorten effective service life. As an example, the Hubble space telescope, a satellite that is on LEO, could have its effective service life shortened from 15 years to 22 months as a result of an increased accumulated ionizing dose caused by a 50-kiloton exoatmospheric explosion.[74]

Virtually all electronic systems in the United States today are potentially vulnerable to HEMP, ranging from televisions to mainframe computers, and from telephone systems to aircraft and satellites.[75] When

HEMP enters a system, it can cause a variety of adverse effects. These include transient, resettable, or permanent upset of digital logic circuits and performance degradation or burnout of electronic components. The collected energy itself can cause malfunction or device failure directly; or it can trigger the system's internal power sources in unintended ways, causing damage by the power sources within the system itself.[76]

This applies to many military communications systems as well. Over time, modern electronic systems have become increasingly vulnerable to HEMP as a result of transistorization and the use of solid-state and integrated-circuit technologies, which operate at very low voltages. Of course, the major issue for vulnerability is the level of the HEMP-induced transients that reach the sensitive electronics.

Systems can be protected by creating a barrier between the EMP field (which can produce short circuit currents in the area of 10 kiloamperes on power transmission lines) and the system to be protected. The most conservative approach is the creation of a "Faraday cage," a completely closed and perfectly conducting shell. This metallic shield will provide absolute protection against virtually any conceivable HEMP threat. The problem, of course, is that the protected system is useless, because it has no input or output capability. The current approach to shielding is based on integral shielding with penetration control, which attempts to provide shielding, yet retains penetrations into the protected area that are managed by surge protectors for input power lines, wire mesh or transparent conductive-film coatings for windows where visibility is required, metal honeycomb for ventilation ports, and conducting gaskets for doors and hatches.

There are also new possibilities on the horizon: silicon carbide, for example, used instead of silicon in semiconductors, is tolerant to a much broader range of both temperature and voltage.[77] Extended systems, such as the integrated electronic banking system across the United States, will always be much harder to protect, since the weakest link in the system will allow entry to other components.

Despite shielding, relatively little of either the commercial or the military world is effectively and verifiably protected. Within the Department of Defense, tactical military communications systems are probably the most vulnerable, followed closely by theater command and control architecture. The threat, of course, extends even farther, to tactical aircraft and, in fact, to *any* system that uses advanced solid-state electronics to

perform basic functions. This encompasses most of the systems in the U.S. military today—from wheeled vehicles to helicopters.[78]

The satellite constellation, both military and commercial, with the exception of certain systems related to the Single Integrated Operation Plan (SIOP), is potentially vulnerable to HEMP. According to one observer, "Quite simply, the use of commercial satellites is now so tightly woven into the fabric of our commercial and military endeavors that the consequences of the loss of these assets is unthinkable, yet such loss is a very real possibility."[79]

What is shielded? The systems related to strategic command and control are protected.[80] The weapons systems associated with SIOP execution are also presumably protected. Not much else is definitely safe. As a general principle, our strategic command and control is better prepared for the potential effects of EMP than are our tactical forces.[81]

While the world of HEMP is little known and even arcane, there is one notable source of serious study and analysis. The Soviet Union embraced HEMP as an integral part of its strategic warfighting concept during the Cold War and devoted a significant part of its strategic order of battle to achieving decisive HEMP effects in a general nuclear war.[82] It is reasonable to assume that others have studied Soviet analyses.

The statement attributed to Indian General Sundarji about the need to have nuclear weapons when confronting the United States does not go far enough—not only are nuclear weapons needed, but also a delivery system capable of lofting a nuclear weapon to an altitude of 100–300 kilometers in a regional battlespace. The ability to do this will threaten to drive a stake through the very heart of the operational principles that drive U.S. warfighting doctrine. We are now, and will be increasingly in the future, reliant on secure information systems to deploy our forces and to employ them effectively in a theater. HEMP threatens at least to disrupt our ability to do this, and at worst to prevent us from developing the "information synergy" fundamental to *Joint Vision 2010 (JV 2010)*. Allies and coalition forces will probably have lower levels of protection than U.S. forces and a commensurately greater risk.

An exoatmospheric nuclear detonation offers a regional state the ability to apply nuclear weapons in a nonlethal application (a 20-kiloton burst at 150 kilometers altitude will produce no visible radiation, blast, or fire effects on the ground) that will still have profoundly disruptive effects on U.S. space, air, ground, and sea operations. It could change the character of a theater war from that of a *Desert Storm* to a Verdun, namely, from

an information-rich environment to one in which fused intelligence will be local in nature and very hard to pass both laterally and vertically. Most importantly, the use of nuclear weapons in this manner avoids crossing the nuclear Rubicon—a direct attack upon U.S. forces that would bring a clear, unequivocal response. A HEMP attack is a sideways swipe that will force the NCA to think long and hard. Is an exoatmospheric nuclear explosion—in which no U.S. personnel die as a direct result—serious enough to warrant a nuclear response against a Baghdad, Tehran, or Pyongyang? Of course, many personnel will be in grave danger after such an attack, even if no one dies from blast, heat, or radiation. Planes and helicopters may fall from the sky, fire control architecture and tactical radios may not work, and vehicles may not move.

Is this an overstatement of the threat? The use of HEMP will affect adversary as well as friendly systems, and those societies that have moved directly to cell phones as their basic communications architecture may be more vulnerable than societies (including some of our potential theater-level adversaries) with modern fiber-optic cabling. Despite this, as a general principle it is reasonable to say that HEMP effects will tend to have more negative effects on organizations that are reliant upon electronics,and that almost uniquely describes the U.S. approach to warfighting—an approach that will become accentuated further as we move into the 21st century.

An attack against the U.S. homeland using HEMP remains the most potentially disruptive and dangerous possibility. An effective attack could cause incalculable consequences, seriously retarding if not reversing U.S. capabilities in the information age. The ability to deliver this kind of attack will require the ability to deliver an intercontinental ballistic missile to an altitude of between 100 and 500 kilometers over the center of the North American continent (or alternatively the orbital placement of a satellite). This is hard to do covertly. The "strategic forensics" will be clear and unambiguous, and a regional actor that chose this option would be risking its very national survival. Unlike the thrust of Soviet Cold War scenarios, national decapitation would be impossible to achieve, and the strategic forces of the nation would be largely protected and available for a response.

Even so, a regional state with the capability to deliver such an attack would possess a qualitatively higher order of deterrence than one limited to regional attack. Several regional powers seem to understand this concept clearly and are working feverishly to develop an intercontinental

missile capability. This remains a less likely but overwhelmingly dangerous alternative. The "panic element" that would attend even a credible threat to launch such an attack would have to be taken into account by U.S.planners in a crisis.

Alternative Operational Concepts

At the end of the millennium, the United States remains intent on harnessing technology as the engine that drives our vision of warfighting. As recently as November 1999, the Commander of the Army Materiel Command, General John Coburn, posited that "The history of warfare is the history of technology."[83] There are many who would disagree with this assertion. Perhaps seduced by our own cultural limitations, we have been slow to recognize that others, either through choice or by necessity, may not follow the same path. A recently released series of interviews on the Chinese book *No-Limit Warfare* quotes one of its authors, Senior Colonel Qiao Liang, as saying "If we were to try to use high technology to counter U.S. high technology, that would in fact land us in the U.S. trap. We could never catch up to them on that track. So for a poor and weak country to try to use high technology to counter the United States would in fact be like throwing eggs against a rock."[84]

In choosing not to compete directly against the United States technologically, other nations can choose to reject the dialectic that is the "Western Way of War." In the operation of the Hegelian dialectic, thesis competes with antithesis, resulting in synthesis, which subsequently incorporates elements of both competing approaches. This approach tends to produce military organizations that converge in doctrine and hardware, mirroring each other to some degree. This convergence is at the very center of Western military history. As Senior Colonel Qiao Liang argues, potential adversaries may make a conscious attempt to reverse this process and avoid mirroring Western military organizations and approaches to war.[85] Clearly, some of this rhetoric is the response of a weaker state that must make the best of the hand it has been dealt, and even the most imaginative alternative operational concepts may not prove effective when called upon to operate against our conventional superiority.[86]

A refusal to adopt Western approaches may go well beyond questions of operational convergence and military effectiveness. The most lucrative potential approach could be to seek advantage by operating well outside the moral framework of the traditional Western approach, rejecting what we see as universal norms of behavior. The writings of Ralph Peters (*The New Warrior Class*) and Charles Dunlap (*How We Lost*

the High-Tech War of 2007) brilliantly highlight these possibilities.[87] Of course, such approaches bring their own limitations and cultural biases in viewing U.S. society and resolve. In particular, there is a widely held view that U.S. society is preternaturally sensitive to even minor casualties, yet recent evidence indicates this may not be so.[88]

Regional aggressors or rogue states may choose to view their populations as assets to be expended, using what has been called the "operational maneuver of starving women and children."[89] If innocent civilians are starving, left exposed to the elements, or attacked in any one of a number of ways available to a modern state, their condition will become of intense interest to the theater commander. The regional commander-in-chief (CINC) will have to take their well-being into account in his operational plans and be prepared to allocate scarce assets to care for them. Anyone who asserts that this will not become a competing priority with ongoing military operations is unfamiliar with the power and political sophistication of nongovernmental organizations (NGOs) and the pressures exerted by the "CNN effect."

Asymmetric actors may also choose to disregard the concept of victory and defeat, illustrated in the conversation between an American and a North Vietnamese officer, Colonel Harry Summers and Colonel Tu, in Hanoi on 25 April 1975: "You know you never defeated us in the field," said Summers. "That may be true," replied Tu, "but it is also irrelevant."[90]

Since the end of the Gulf War, Saddam Hussein has attempted to execute just such a strategy, whereby, over time, just remaining in the game against a superpower, regardless of the beating his forces are taking at the hands of *Northern Watch*, has conferred political credibility in many parts of the world (not least of all, in Iraq).

The Iraqis may understand Clausewitz better than we do: "War, however, is not the action of a living force upon a lifeless mass (total non-responsiveness would be no war at all), but always the collision of two living forces. The ultimate aim of waging war must be taken as applying to both sides. Once again, there is interaction. So long as I have not overthrown my opponent I am bound to fear he may overthrow me. Thus, I am not in control; he dictates to me as much as I dictate to him."[91]

Tactical Employment

While a combination of technological approaches and innovative tactics can be used against U.S. forces, the best counter of all may rest in battlespace selection. If an opponent can force the fight to complex urban, mountain, or jungle terrain, U.S. sensors and weapons accuracy

will be degraded, and the potential for U.S. casualties will rise. Choosing the right ground may well prove to be the most significant advantage resting with an adversary, and U.S. forces may not be able to refuse to enter these killing grounds.[92]

Other supporting tactical asymmetric approaches can include the use of the civilian population as hostages, as human shields, and as weapons with which to overstress U.S. and allied medical systems. All of these factors will tend to reduce the effectiveness of precision engagement systems, clouding the picture of the battlefield, and requiring greater exposure by U.S. forces. If nothing else, they always invite the opportunity for tactical mistakes, which an effective information operations campaign would then turn to great effect. On the other hand, it is important to recognize that positive tactical results may have negative strategic implications. The event itself may be of less importance than how it is presented on the global stage.

Operational Employment

The use of antiaccess concepts can deter, slow, or prevent U.S. forces from entering an AOR. The technologies for antiaccess are not new, but how they are employed and "advertised" will determine effectiveness. They range from high-tech to low-tech, from conventional sea-based mines to shoulder-fired surface-to-air and surface-to-surface missiles (SAMs and SSMs). When combined with unfavorable terrain, and against a backdrop of low to moderate U.S. interest, these approaches may gain powerful advantage. They will tend to be less effective when a vital U.S. national interest is at stake.

Antiaccess measures can be grouped into four broad and overlapping categories: deterring measures, coercing measures, antideployment measures, and anti-invasion measures. They can be either conventional or WMD. While the specifics of potential WMD antiaccess measures have been covered in detail earlier in this chapter, they will also be briefly discussed in this section, since they represent the "high end" of access denial.

Deterring measures are those actions and systems that are designed to prevent the United States or our allies from deploying forces or other forms of politico-military assistance to a region in a crisis. This would be accomplished through a display of force or diplomacy that makes the cost of the proposed action appear too high, when considered against the level of U.S. national interest at stake. These normally are pre-hostility measures, although deterrence can operate even after a conflict begins.

The display of military hardware and the calibrated use of rhetoric about potential employment would be deterring measures. The backdrop to this would, of course, be the adversary's calculations about the level of U.S. national interest at stake, balanced against the contemplated action. The availability of WMD, and more particularly, the demonstrated ability to deliver a WMD attack against the continental United States, would probably be the highest expression of this form of deterrence.[93]

Coercing measures combine military threat and diplomacy and are aimed at regional states to cause them to refuse or limit U.S. basing or deployment. This is the implicit or explicit capability and resolve to strike at nations within a region that would be necessary to support the deployment of U.S. and allied forces. The highest expression of this form of coercion would be the possession of ballistic missiles that could reach population centers of the countries in question, coupled with WMD. Less obvious but equally effective operational capabilities would include a credible SOF threat for employment of WMD, surface-to-surface cruise missile threats, the ability to interdict economically critical lines of communication, and the potential to incite destabilization operations against the regime in power. There are many more. In fact, virtually any weapon or technique discussed below can be employed to this end. The ultimate intent is to drive a wedge between regional and extra-regional states (presumably the United States with its allies) by demonstrating that the cost of siding with America will be too high.

Antideployment measures are the military weapons systems and the tactics, techniques, and procedures, both active and passive,that could be employed to prevent or slow the deployment of U.S. and allied forces by air or sea to friendly ports and debarkation airfields in an AOR. They are also the measures undertaken against forward-deployed U.S. Navy and allied warships to deny or limit their freedom of movement and action in contiguous ocean areas.

Anti-invasion measures are the military weapons systems and the tactics, techniques, and procedures, both active and passive, employed to deny U.S. and allied forces the capability to execute sea control, amphibious, airborne, air assault, air superiority, and air-to-ground missions within an AOR. Many of them are the same systems and tactics that are used for antideployment, but there are some significant differences. The principal difference is that the state in question is now defending its own

Table 2. Conventional antideployment approaches

Conventional antideployment weapon or tactic	Prevents, limits, or denies what U.S. capability?	Benefits	Risks
Tether, bottom, rising mines	■ Ability to move forces by sealift ■ Naval freedom of action	■ Cheap, highly effective ■ Reasonably deniable	■ Must be placed at selected target area
Free-floating mines	■ Ability to move forces by sealift ■ Naval freedom of action	■ Cheap ■ Highly deniable	■ Indiscriminate ■ Not responsive to retasking or redeployment
Surface-to-air missiles	■ Ability to utilize aerial ports of debarkation (APODs) ■ Air freedom of action	■ Cheap ■ "High leverage" technique if special operations forces employed against targeted APODs	■ Operationally difficult to employ in target nation—possibility of attribution
Submarines	■ Ability to move forces by sealift ■ Naval freedom of action	■ Effective ■ "High leverage" technique ■ More effective as a threat than as an actual weapon ■ Very discriminate	■ Clearly attributable ■ Expensive ■ Probability of loss high
Cruise missiles	■ Ability to move forces by sealift ■ Naval freedom of action ■ Ability to use APODs	■ Cheap ■ Discriminate ■ High coercive value	■ Limited range—geographically dependent ■ Limited effectiveness against modern navies ■ Clearly attributable
Theater ballistic missiles (conventional warheads)	■ Ability to move forces by sealift ■ Naval freedom of action ■ Ability to use APODs	■ Very high coercive value ■ Difficult to counter ■ "High leverage" threat that will require disproportionate resources in air assets to counter	■ Limited effectiveness against sea-based targets ■ Clearly attributable ■ Expensive
Tactical aviation	■ Ability to move forces by sealift ■ Naval freedom of action ■ Ability to use APODs	■ Discriminate ■ "High leverage" technique—Can be very effective against "air bridge"	■ Clearly attributable ■ Operationally difficult to execute ■ Probability of loss very high if employed

(continued)

Table 2. Conventional antideployment approaches *(continued)*

Conventional antideployment weapon or tactic	Prevents, limits, or denies what U.S. capability?	Benefits	Risks
Special operations forces	■ Ability to use infrastructure in host country	■ Discriminate ■ Deniable ■ High leverage	■ Possibility of compromise and loss of deniability ■ "Diminishing returns" as security responds
Artillery systems	■ Ability to use sea- and aerial ports of debarkation	■ Cheap ■ Discriminate	■ Very limited range ■ Geographically dependent ■ Clearly attributable

[1] See John Stillion and David Orletsky, *Airbase Vulnerability to Conventional Cruise-Missile and Ballistic-Missile Attacks: Technology, Scenarios, and U.S. Air Force Responses* (Santa Monica, CA: RAND, 1999).

borders and the area it may have invaded, instead of projecting power into neighboring states (although this will surely continue).

In addition to the capabilities outlined above, certain backbone or enabling capabilities are highly desirable. These include, first, a space-based reconnaissance capability, either indigenous, through relationships with states that do possess military space systems, or through commercially available systems; and second, a comprehensive reconnaissance-strike complex able to conduct reconnaissance, process information, develop intelligence, and execute a strike plan based on these.

Understanding the distinction about the level of U.S. national interest at stake is fundamental to analyzing antiaccess approaches. If the United States seeks access and a vital national interest is at stake, then it will be difficult to stop us. The loss of a carrier or a number of B–2 bombers, for example, might be acceptable—if the objective is important enough. Conversely, the threat of losing a carrier or a large number of manned aircraft may be enough to deter the United States in situations where our interest is very low. There is also a hidden and dangerous dynamic at work for the state that makes these calculations—a shocking and successful attack on a U.S. asset may well prove to be the catalyst that drives U.S. interest to a far greater level than it might have otherwise been. These calculations of deterrence will need to be very carefully undertaken by potential foes, and the risks of getting it wrong are substantial.

Table 3. Conventional anti-invasion approaches

Conventional anti-invasion weapon or tactic	Prevents, limits, or denies what U.S. capability?	Benefits	Risks
Passive measures (cover and concealment, vertical and horizontal engineering, and the development of defensive ground tactical positions in depth)	■ Ability to execute cross-beach amphibious assaults, airborne landings, air assault landings, and air interdiction and close air support	■ Can deter and perhaps limit planning for forcible entry operations ■ Relatively cheap	■ Usually not effective ■ Fixed and immobile ■ Can be breached or avoided
Surf zone mines	■ Ability to execute amphibious operations	■ Can deter and perhaps limit planning for forcible entry operations ■ Relatively cheap	■ Fixed and immobile ■ Can be breached or avoided
Tether, bottom, rising mines	■ Ability to move forces by sealift ■ Naval freedom of action	■ Cheap ■ Highly effective	■ Must be placed at selected target area ■ May be difficult to place against a capable navy executing sea control tactics
Free-floating mines	■ Ability to move forces by sealift ■ Naval freedom of action	■ Cheap	■ Indiscriminate ■ Not responsive
Surface-to-air missiles	■ Ability to execute aerospace tasks	■ Relatively cheap	■ Countermeasures readily available ■ Use invites counterattack ■ Cannot offer a decisive result
Submarines	■ Ability to move forces by sea ■ Naval freedom of action	■ Effective ■ "High leverage" technique ■ More effective as a threat than as an actual weapon	■ Expensive ■ Probability of loss high
Cruise missiles	■ Ability to move forces by sea ■ Naval freedom of action ■ Ability to use aerial ports of debarkation	■ Cheap	■ Limited range ■ Geographically dependent ■ Limited effectiveness against modern navies

(continued)

Table 3. Conventional anti-invasion approaches *(continued)*

Conventional anti-invasion weapon or tactic	Prevents, limits, or denies what U.S. capability?	Benefits	Risks
Theater ballistic missiles (conventional warheads)	■ Ability to move forces by sealift ■ Naval and aviation freedom of action ■ Ability to use APODs	■ "High leverage" asset that will require U.S. and allies to counter with a large number of critical air, space, and special operations assets ■ Effective counter may not be available	■ Limited effectiveness against sea-based targets
Tactical aviation	■ Ability to move forces by sealift ■ Naval freedom of action ■ Ability to use APODs	■ Discriminate ■ "High leverage" technique ■ Can be very effective against "air bridge" ■ Possibility of single "high value" attack	■ Operationally difficult to execute ■ Probability of loss very high
Artillery systems	■ Ability to execute forcible entry by air or sea	■ Cheap	■ Limited range ■ Geographically dependent ■ Limited effectiveness ■ Easily targeted

The integration of the various antiaccess asymmetric approaches that use both the diplomatic and military elements of power and both conventional and WMD means can give a clear picture of the range of alternatives available to a state to execute a comprehensive antiaccess strategy, with all its operational and tactical enabling approaches.

Strategic employment on the tactical level that is well beyond accepted norms (such as the state-sanctioned raping of captive U.S. servicewomen depicted by Charles Dunlap in *How We Lost the High Tech War of 2007*) can have direct strategic application on either softening or hardening U.S. national will. Some defense thinkers take the position that such potential future atrocities would have a softening effect.[94] This is not an uncontested hypothesis; Americans both in and out of uniform may prove resilient in the face of warrior tactics.[95]

Table 4. Summarizing antiaccess measures

Antiaccess approach	What is the goal of the approach?	When will it be employed?	Who is the target?	What is the "low end"	What is the "high end"
Deterrence	Prevent or limit U.S./allied *involvement* in a crisis	During peace and early in a crisis	U.S. and allies	Diplomatic contacts, "saber-rattling"	Overt threat of weapons of mass destruction (WMD) employment against U.S. forces, allies, and the continental U.S.
Coercion	Prevent, limit, or deny *access* for U.S./allies in a crisis	During peace and throughout a crisis	Regional states	Economic, military-to-military, diplomatic pressures	Overt threat of WMD employment against targeted regional state
Anti-deployment	Prevent, limit, or deny *deployment* of U.S./allied forces in a crisis or war	Early in a crisis	Regional states and U.S. strategic deployment system, to include sea-based forces and air and sea ports, including potential intermediate staging bases (ISBs) in range	Mines	WMD employment against regional states and U.S. strategic deployment system, to include sea-based forces and air and sea ports and ISBs
Anti-invasion	Prevent, limit, or deny *forcible entry* of U.S./allies in a war	Mid- and late-crisis	U.S. and allied tactical forces and supporting infrastructure	Mines, surface-to-air missiles, air defense artillery, passive protection	WMD employment against regional states and U.S./allied forces strategic deployment system, to include sea-based forces and air and sea ports and ISBs

Our conventional superiority may well roll through the warriors, just as the troops of the 2d Marine Division rapidly breached the trenches of Iraqi infantry forces during Operation *Desert Storm*. Technology may well prove the equal of fanaticism.

The possibilities inherent in alternative operational concepts cross the levels of war and are tightly wound into a cycle of action-reaction with potential U.S. counters. For this reason, it is necessary to discuss some United States concepts and operational constructs while examining this form of asymmetry. Two arguments active among U.S. defense thinkers today must be considered. The first is concerned with the types of forces and the operational approaches that the United States should adopt in the face of the growing WMD and access-denial threat. The second deals with how we should deal with the vast areas of urban complex terrain that are expanding to cover much of the populated world. This terrain presents a dramatically more difficult operational environment for U.S. forces, who have long avoided fighting in cities when they have had the choice.

The WMD and antiaccess argument: This argument asserts that the lethality of theater ballistic missiles, armed with various WMD, will make it precarious to deploy ground, naval, and tactical air forces to a theater in a crisis.[96] The potential gain we will enjoy from their deployment will be offset by the vulnerability that attends their presence in the theater within range of enemy weapons. The alternative? More cruise missiles and strategic bombers deploying directly from the continental United States or other distant regional bases and armed with precision weapons and other standoff munitions.

This argument has some attractions, to be sure. If our ground, naval, and tactical air forces aren't there, then they can't be attacked. The problem with this approach is that it ignores the shaping component of the national military strategy by drawing down on forward-deployed forces. We deploy forces forward on permanent and rotational bases in order to demonstrate interest, build closer ties to friends, and demonstrate resolve to potential enemies. This approach would largely ignore this vital component of current U.S. strategy, and substitute for it something more akin to "Fortress America." This would be a "New Look" for the early decades of the 21st century that would, in fact, share many of the disadvantages of the Eisenhower administration's strategy. The most notable similarity is a lack of flexibility and a very limited capability to apply

discriminate measures tailored to specific situations below the threshold of employment of WMD. This is an example of worst-case planning driving all other scenarios, even those that are far more likely to occur. It also minimizes the large number of actions that can be taken by forward-deployed forces both in peacetime (as part of a CINC's Theater Engagement Plan, or TEP) and in crisis.

The avoidance of cities: It is vital to recognize that there are places—the "dark and bloody ground"—where U.S. forces will need to be able to fight and prevail. It will not always be possible to engineer scientific and technical solutions to all of these problems. There is a trend, based on our love affair with technology, that may lead us to seek to avoid going into environments—particularly urban complex terrain—that will tend to degrade and minimize our maneuver, firepower, and information advantage. This could lead us to develop powerful yet brittle forces that cannot prevail across the potential spectrum of engagement. At a minimum, it would invite obvious asymmetrical responses to an overwhelming yet narrowly based conventional advantage.

It has been argued that we should surround complex terrain, and then let cities "wither on the vine."[97] Unfortunately, we will not always have the luxury of doing this. As the bank robber said when questioned about why he robbed banks: "Well, that's where the money is." Cities are the centerpiece of virtually all cultures, both east and west, and the growing urbanization of the world means that we must learn to master the skills required to prevail in this environment.[98] This is not a refutation of technology, for the answer to the problem will require the most sophisticated and capable technology available—but it is ultimately a problem of human will and skill. Our potential opponents see this; we should not ignore it.

The Army, Marine Corps, and Air Force are studying the problem of urban warfighting: the Army through a series of Advanced Concept Technology Demonstrations (ACTDs) and the Marine Corps through its *Urban Warrior* series of experiments. The Air Force is studying the role of airpower in the urban environment.[99] While none of the series of experiments or research to date has yielded a breakthrough idea for success in the dangerous urban environment,many small and very cheap incremental improvements have been identified.

The need to master the urban environment may be more important in small-scale contingencies (SSCs) than in major theater wars. In a major theater war, the theater commander may have the luxury of being able to maneuver away from urban terrain while achieving his objectives.

In an SSC, many of the most likely scenarios for the employment of U.S. forces will require entry into urban complex terrain—we will not be able to pick and choose where evacuations, embassy reinforcements, and humanitarian operations will occur.

What does this mean? As we design the forces that will execute the national military strategy, we need to avoid creating forces effective against a band of scenarios too narrow and optimistic, overly reliant on technology.[100] In some future war we do not want to find ourselves in the position RAF Bomber Command found itself in 1942: unable to effectively attack critical targets, the RAF attacked the city of Lubeck because it would burn well, rather than for any significant operational consideration.[101]

Terrorism

Terrorism is included in this matrix of threats even though it is an uncomfortable fit. Terror can be a means chosen by a state actor, and in that interpretation, it fits more or less into all of the previous categories. For this categorization, though, the intent is to highlight the danger of nonstate sponsored groups that operate outside the framework of international relations. Their financial and scientific base will be narrower than state-sponsored organizations, but this is compensated for by their readiness to select more radical techniques that would be suicidal for groups linked to states.

As has already been highlighted, the rise of the United States as the global lightning rod for everything that happens in the world today tends to attract would-be attackers. The global reach of American culture only reinforces this. When coupled with the growing availability of weapons that promise massive and visible results with minimal outlay, the potential for nonstate actors to invoke weapons formerly reserved for states is clear and growing. The Cold War formula of "least likely = most dangerous" is fast eroding, and many unsavory scenarios can be imagined that are all reasonably likely to occur.

The Who: Regional, Rogue, and Nonstate Actors

A peer competitor is the least likely opponent to emerge within the time frame of this analysis (through 2010). For this reason, it is not included here.A regional adversary[102] is possible, and even likely. The representative goal of such a regional opponent would be the pursuit of regional hegemony. The United States would most likely face this adversary in a coalition of some form. An opponent of this nature could reasonably

expect some limited international support, which would tend to narrow asymmetric options—at least from the more egregious WMD and warrior alternatives.

Few if any inhibitions will act to brake the asymmetric strategies selected by a rogue state. Such a state can expect to act with little or no international support, so there is less incentive to avoid extremes of behavior. At the same time, such a state may gamble that the only way to gain international support will be by self-inflicted attacks, coupled with an aggressive strategic IW campaign that would attempt to pin the blame for such an attack on the United States and its allies.

The nonstate adversary spans a very broad variety of threats, ranging from the most plausible (handbills nailed to telephone poles) to extreme (anthrax releases in subway stations). For this reason, generalizations about these organizations are difficult.

In examining potential adversaries, the more ties a state has to the existing international community, the less likely such a state will be to select an asymmetric strategy that would place it beyond the pale of the society of nations. This can be restated in another manner: the more a state has to lose,the less likely it will be to adopt a strategy that could produce unlimited liability if unsuccessful.

The When: Likelihood During Phases of a Crisis

Table 5 presents the relative likelihood of different potential opponents choosing to employ asymmetric approaches as a function of time. The opponents—regional, rogue state, and nonstate actors—are arrayed down the left-hand column. Within each row are arrayed the most likely forms of asymmetric alternatives that have already been discussed (nuclear, chemical, biological, information operations, operational concepts, and terrorism). The five columns represent the potential phases of a crisis. Each phase would present distinctly different options and alternatives for an adversary to consider the use of an asymmetric approach. Peace represents a noncrisis state of international relations in which there is no particular focus on a state or region. A crisis represents a heightened state of diplomatic focus on a particular state or region, including potential alliance or coalition diplomatic mobilization. Deployment is the movement of U.S. and allied forces to an AOR. Employment is the execution of combat operations in an AOR. The deployment and employment phases may overlap. Termination represents the endgame of a major theater war or small-scale contingency; for purposes of this

Table 5. A question of timing: relative likelihood of asymmetric use during phases of a crisis

Opponent	Asymmetric Option	Phase of a Crisis				
		Peace	Crisis	Deployment	Employment	Termination
Regional						
	Nuclear	Lowest	Lowest	High	Low	**Highest**
	Chemical	Lowest	Low	**Highest**	High	Low
	Biological	Lowest	Low	**Highest**	Low	High
	Information Operations	High	**Highest**	High	High	High
	Operational Concepts	N/A	N/A	High	**Highest**	Low
	Terrorism	High	**Highest**	High	High	High
Rogue State						
	Nuclear	Lowest	High	**Highest**	Low	High
	Chemical	Lowest	High	**Highest**	High	High
	Biological	Lowest	Low	**Highest**	Low	High
	Information Operations	High	**Highest**	High	High	High
	Operational Concepts	N/A	N/A	High	**Highest**	Low
	Terrorism	High	**Highest**	High	High	High
Nonstate						
	Nuclear	Lowest	Low	**Highest**	High	High
	Chemical	Lowest	Low	**Highest**	High	High
	Biological	Lowest	Low	**Highest**	High	High
	Information Operations	**Highest**	High	High	High	High
	Operational Concepts	N/A	Low	High	**Highest**	Low
	Terrorism	High	**Highest**	High	High	Low

analysis it is assumed that the termination is occurring on terms favorable to the United States and its allies.

The relative likelihood of employment ranges from lowest to highest. When reading this table, it is important to understand that this is not an attempt to make a judgment on when an asymmetric strategy might be best used; rather, it simply indicates at what stage an adversary might be more likely to select an asymmetric approach.

Several conclusions emerge from this table. First, WMD are "bookend" options. They are more likely to be useful either as coercing measures or as actual weapons at the very beginning or the endgame of a conflict. At the beginning, even the threat of their employment may slow or stop U.S. deployment into a theater. A lesser-included outcome of this will be the political fragmentation that can occur among a coalition structure when faced with such a scenario, particularly when there are widely disparate levels of NBC preparedness among allies. At the end of a major theater war or small-scale contingency that is going badly for the aggressor, the temptation will be to "use 'em or lose 'em," and this will be more pronounced if there is a chance of regime replacement. The more decoupled a state is from the international community, the more pronounced the possibility of a blind and potentially disastrous use of WMD.

Second, it is very hard to draw conclusions about how a nonstate actor might choose to time the employment of asymmetric alternatives, but the activities of a regional actor or a rogue state might increase the opportunities for a nonstate actor to conduct operations. It is conceivable that such an operation might be intended to have a "false flag" effect that would prompt the United States to take action sought by the nonstate actor against a regional opponent.

Third, the specifics of the situation will always carry more weight than any generalized theory. In particular, this applies to the category of concept-based asymmetric approaches. Terrain, cultural considerations, and the level of national interest at stake are ultimately of more importance than anything else in determining these relationships.

Conclusions

Two principal conclusions can be drawn from this examination of the what-who-when of asymmetry. First, a number of potential adversaries are exploring strategies, the most dangerous and threatening of which are usually based on the acquisition of WMD, that may narrow certain gaps with the United States, but at a potential grave overall cost

to their own states. These strategies also tend to produce unbalanced militaries that cannot function effectively in a traditional manner, as they focus on the asymmetric approaches that seem to offer the most promise of fast results against the United States and its allies.

The second observation deals with the relative importance of weapons of mass destruction within the typology of asymmetry. It is inviting to reduce the asymmetric argument to a discussion of the strategic WMD threat to the United States homeland. This is a dangerous oversimplification, because, while it captures the most destructive and frightening end of the asymmetric spectrum, it also ignores a number of far more likely applications of asymmetry. Weapons—regardless of the type—are themselves of less importance than the effect they create in the mind of the attacked. There is a powerful congruence, to be sure, between WMD and immediate strategic effect, but there are also other, less dangerous ways to achieve similar effects. We should not limit our thinking about how to defend against asymmetric approaches to too narrow a band that encompasses only the most dangerous.

Chapter Three

Looking in the Mirror: Where Are Our Asymmetric Vulnerabilities?

Any sufficiently advanced technology is indistinguishable from magic.[103]

—Clarke's Third Law, Arthur C. Clarke, *Profiles of the Future*

The people who can destroy a thing, they control it.[104]

—Frank Herbert, *Dune*

The central thesis of this paper is that the Department of Defense's portion of U.S. national policy in the near to mid-term is based on the ability to maintain a clear and unambiguous conventional military superiority, coupled with the ability to defend the homeland in the face of potential asymmetric threats. This chapter will outline the conceptual structure of both U.S. military operations and the most important physical and psychological elements of our homeland. Potential vulnerabilities within these concepts and structures will be described and examined. At the end of the chapter, some conclusions will be offered that will establish the groundwork for chapter four, which will assess the danger of possible asymmetric attacks on the United States and its forces.

Measuring Conventional Military Superiority

U.S. conventional superiority is embodied in the capability to rapidly achieve overwhelming battlespace dominance against any opponent, and to prevail quickly and with acceptable loss. It draws its doctrinal codification from the "big four" concepts of *JV 2010,* the Chairman's vision of the future battlefield: dominant maneuver, precision engagement, full dimensional protection, and focused logistics. These overarching concepts are useful at the macro level, but we need to look at what they mean on the ground. Is it possible to establish some relative measures of

effectiveness for how the doctrinal concepts are expressed operationally? If so, can we then consider some possible vulnerabilities to asymmetric approaches? The answer to both questions is a qualified yes.

What Are the Operational Expressions of *JV 2010* Capabilities?

Dominant maneuver achieves its goals through four enablers. First, information superiority creates a common picture of the battlespace while denying the same to the enemy. Second, highly capable and agile combat units are employed to use this degree of information superiority to strike enemy forces at the most advantageous time and place, in both a close and deep battle. Third, forces are deployed rapidly both inter- and intratheater, integrating rapidly with forward presence forces to fight. Fourth, objectives are achieved whenever possible through the manipulation of effects, not through the application of mass. The measures of effectiveness will be whether or not CINC objectives can be met through, first, rapid operations that yield decisive results; second, acceptable U.S. and allied casualties; and third, acceptable collateral damage. In *Desert Storm*, the great "left wheel" of the coalition is a good example of an effective application of dominant maneuver.

Precision engagement achieves operational expression through three key enablers. First, information superiority is used to rapidly exchange targeting information among multiple sensor platforms, process information into actionable intelligence, and then convey it to the shooter in near-real-time. Second, multiple sensor systems, both manned and unmanned, surveil the battlespace. And third, effects-based targeting is applied. The measure of effectiveness will be whether we can conduct effective engagements that meet CINC targeting goals with acceptable collateral damage and U.S. and allied casualties. As with all measures of effectiveness, this remains a qualitative judgment, the most important component of which will be the CINC tolerance for error.

Two counterpoised examples from history illustrate this. In preparing for the invasion of France in 1944, the decision was made to attack the transportation system that would be used to move German reinforcements to the lodgment area. This involved a conscious decision to target railyards and switching facilities inside French towns. Early civilian collateral casualty projections were quite high, but General Eisenhower considered the potential gain worth the risk. As it turned out, casualties were much lower than projected, and the "Transportation Plan" greatly slowed the movement of German units. More recently, though, in Operation *Desert Storm*, the bombing of the al Firdos command and control

bunker in Baghdad, a legitimate military target that contained a number of Iraqi civilians, proved to be "too much for the traffic to bear," and subsequent strikes were modified and the force of the air campaign lessened.[105] The difference in what degree of error a CINC was willing to accept (or allowed to accept because of pressing diplomatic realities) was vastly different in these two cases. This is ultimately an expression of whether the nation's vital interests are at stake.

Full dimensional protection gains its operational expression through two key enablers: the use of information superiority to rapidly exchange information concerning the current threat to U.S. and allied forces, including the ability to protect our own information systems, and the ability to provide effective and timely force protection measures, active, passive, and preemptive, when required. The measures of effectiveness that will determine how well full dimensional protection is being executed are simple: the force deploys,fights, and redeploys with minimum U.S. and allied casualties. This is a qualitative measurement. The number of casualties that will be acceptable will of course be scaled against the nature of the threat and whether or not vital interests are at stake. Two extreme cases from history would be the invasion of Normandy in 1944, and the invasion of Grenada in 1983. Normandy involved the survival of the nation; Grenada did not. The relative price the United States was willing to pay was significantly different in each of these two scenarios.

Focused logistics operates through three enablers. First, information superiority allows the broad-based sharing of a common picture of the force's logistics posture, while protecting this critical information from compromise. Second, smaller, highly responsive logistics elements will be tailored to provide timely support, with the added benefit of reducing the logistics footprint and the concomitant need for force protection. Third, logistics support will use highly mobile organizations capable of sustained operations at a very high tempo. The measure of effectiveness will remain the one against which logisticians have been measured for centuries: operational tempo does not degrade because of logistics bottlenecks or slow throughput.

The key to all aspects of *JV 2010* is the absolute requirement to dominate the information warfare spectrum. *JV 2010* is ultimately nothing more than a form of what the Navy calls "network centric warfare," a broader concept that explicitly places the full spectrum management of information at the core of a vision of integrated air, space, land, and sea combat.[106]

Where Are the Vulnerabilities in *JV 2010*?

There are vulnerabilities that an intelligent opponent can exploit. Table 6 outlines several measures that could be applied against each of the capabilities and their operational expressions. In general, though, potential effective asymmetric approaches seem to have the following common characteristics when arrayed against *JV 2010*:

- Deny rapid and decisive action through battlespace selection and denial of timely access (including environmental manipulation if necessary)
- Maximize opportunities for collateral damage
- Fight a very aggressive IW campaign that aims directly at disproportionate effect
- Use the civilian population to stress U.S. theater infrastructure
- Avoid effective targeting through passive, active, and disruptive measures
- Inflict mass casualties when possible
- Complicate U.S. logistics by reducing usable infrastructure
- Lengthen operations: time is the friend of the weak and the enemy of the strong; an adversary who just stays on his feet against the United States and a coalition will eventually gain credibility, regardless of the tactical/operational picture.

The United States military is a fearsome force to be reckoned with. It possesses many strengths, not the least of which is the ability to adapt rapidly to new and demanding conditions. All of the asymmetric approaches above have been tried at one time or another against U.S. forces, and most of them have failed. However, we are not invulnerable.[107] A student of our style of war who seeks to distill our vulnerabilities to a basic common denominator would seek to reduce our ability to dominate the information spectrum while increasing our casualties—all while stretching the engagement out over a long period of time.

Examining the Homeland

The preceding section examined threats to the military forces of the United States. This section will attempt to analyze the most fundamental responsibility of any state: the ability to protect its citizens in their homes from attack. The United States has not suffered a serious conventional attack on its homeland by another state since the War of 1812.[108] On the other hand, the U.S. homeland has been threatened several times. As has been previously discussed, in World War II, Japan attempted, with

Table 6. Measuring the effectiveness of *JV 2010* concepts and some potential asymmetries

Conventional capability	Operational expression	Measure of effectiveness	Potential asymmetric approach
Dominant maneuver	■ Information superiority ■ High-capability combat units ■ Force projection ■ Achieve objectives through manipulation of effects, not mass	■ Rapid, decisive operations ■ Acceptable U.S./ allied casualties ■ Minimal collateral damage	■ Deny access ■ Slow deployment ■ Lengthen operations in time ■ Avoid decisive engagements ■ Maximize U.S. casualties ■ Exploit alliance weaknesses
Precision engagement	■ Information superiority ■ Reconnaissance, surveillance, and target acquisition ■ Effects-based	■ Effective engagements that meet CINC targeting goals with acceptable collateral damage and U.S./allied casualties	■ Deny effective targeting; seek to maximize U.S. casualties and publicize all collateral damage opportunities through aggressive information operations
Full dimensional protection	■ Information superiority ■ Protect forces, facilities, and lines of communication from continental U.S. to theater	■ Acceptable U.S. and allied casualties during force deployments, combat, and redeployment	■ Drive fight to ground that minimizes advantages of U.S., and seeks to lengthen fight and cause maximum U.S./allied casualties
Focused logistics	■ Information superiority ■ Smaller, responsive in-theater footprint ■ Sustained high-speed mobile capabilities	■ Operational tempo not degraded because of logistics bottlenecks or slow throughput	■ Seek to reduce usable infrastructure to stress logistics system ■ "Operational maneuver of women and children"

little success, to float incendiary weapons on balloons into the Pacific Northwest, and the end of the war cut short its plans to conduct biological weapons attacks on the United States. Germany also had plans for long-range bombers and successors to the V–2, but none were developed before Germany fell. During the long decades of the Cold War, Soviet missiles were targeted against both U.S. cities and military installations; in

1962, Nikita Khrushchev took the world to the brink of nuclear war in Operation *Anadyr* by placing SS–4 ballistic missiles in Cuba.

There have been several nonstate attacks on the U.S. homeland since the end of the Cold War. The most spectacular from an external nonstate source was probably the January 1993 bungled attempt by Islamic extremists to blow up the World Trade Center in New York. The most deadly attack was the result of an internal nonstate actor: the bombing of the Murrah Federal Building in Oklahoma City in April 1995 by a fragmented antigovernment group.

Threats to the homeland are not new. Two new elements, however, are our preeminent position in the world today and the accelerating collapse of strategic depth that began with the development of the airplane and was further aided by the development of space as a medium of war, peace, and commerce. Most importantly, though, the explosion of information technologies has negated many of the physical concepts of security that have traditionally defined how states view themselves.

Combined with this smaller and more volatile world is the dramatically increased availability of WMD and other technologies that can create mass disruption, if not destruction, of a society like America's that is heavily reliant upon information management systems.

Quantifying the Homeland: What Are the Targets?

By building on the work done by the President's Commission on Critical Infrastructure Protection, ten critical targets have been identified. The commission identified these eight: the transportation infrastructure, the oil and gas production and storage infrastructure, the water supply infrastructure, the emergency services infrastructure, the banking and finance infrastructure, the electrical power infrastructure, the information and communications infrastructure, and the government services infrastructure. For purposes of this study, the defense infrastructure was added to these eight. Finally, to ensure a focus on the ultimate goal of our national infrastructure—to provide services to the people of the United States—a separate category was added as the tenth potential target: the population of the United States itself. These infrastructures provide the services necessary for our well-being and way of life, ranging from the control of our civil airspace to the coordination of local emergency services and the maintenance of our system of commerce and banking.

Table 7. What's the homeland? Breaking it out[109]

Target	Critical component	Measure of effectiveness	Potential asymmetric approach
Transportation infrastructure	■ National airspace system ■ Airlines, aircraft, airports ■ Roads and highways ■ Trucking and personal vehicles ■ Ports, waterways, vessels ■ Mass transit (rail and bus) ■ Pipelines (natural gas, petroleum, other hazardous materials) ■ Freight and long-haul passenger rail ■ Delivery services	■ Air traffic flows safely and on or near time ■ Mass transit operates efficiently, without lengthy delays ■ Hazardous materials conveyed safely and efficiently ■ Roads operate safely and with minimum to moderate delays in central urban areas ■ Freight carrier systems operate safely and efficiently	■ Physical attack using weapons of mass destruction (WMD) or traditional terrorist means ■ Information warfare (IW) attack aimed at disruption of operating systems (including electromagnetic pulse)
Oil and gas production and storage infrastructure	■ Production, holding facilities, refining and processing facilities, pipelines, ships, trucks, and rail systems for the processing and distribution of natural gas, crude and refined petroleum, and petroleum-derived fuels	■ Production, storage, and distribution systems operate efficiently and safely without intrusion into the public domain	■ Physical attack using WMD or traditional terrorist means ■ IW attack aimed at disruption of operating systems
Water supply infrastructure	■ Sources of water, reservoirs, holding facilities, aqueducts, other transportsystems including pipelines, cooling systems, and other delivery mechanisms ■ Filtration, cleaning, and treatment systems ■ Systems for dealing with water runoff, waste water, and firefighting	■ Water availability remains assured ■ Water for emergency services is available	■ Covert attack with chemical or biological agents ■ Physical attack using WMD or traditional terrorist means ■ IW attack aimed at disruption of operating systems ■ Simple contamination

(continued)

Table 7. What's the homeland? Breaking it out[109] *(continued)*

Target	Critical component	Measure of effectiveness	Potential asymmetric approach
Emergency services infrastructure	■ Medical, police, fire, and rescue systems and personnel	■ Emergency systems and personnel are readily available ■ Emergency system is not overtaxed by requirements	■ Physical attack using WMD or traditional terrorist means ■ IW attack designed to increase friction in command and control systems ■ Overstress capability to respond by the scope of the potential event
Banking and finance infrastructure	■ Retail and commercial organizations, investment institutions, exchange boards, trading houses, reserve systems, including associated operational organizations, government operations, and support activities ■ Storage, investment, exchange, and disbursement functions	■ Monetary systems are protected and physical and electronic safety do not become an issue in public domain	■ IW attack aimed at disruption of operating systems, to include electronic theft ■ Physical attack using WMD or traditional terrorist means
Electrical power infrastructure	■ Generation stations ■ Transmission and distribution networks ■ Transportation and storage of fuel essential to this system	■ Electricity is available with minimal disruptions	■ Physical attack using WMD or traditional terrorist means ■ IW attack aimed at disruption of operating systems
Information and communications infrastructure	■ Computing and telecommunications equipment, software, processes, people ■ Processing, storage, transmission of data and information ■ Processes and people that convert data into information and information into knowledge ■ Data and information themselves	■ Information technology systems function with minimal disruptions ■ Data is not lost or irreversibly damaged	■ IW attack aimed at disruption of operating systems (including electromagnetic pulse) ■ Physical attack using WMD or traditional terrorist means

(continued)

Table 7. What's the homeland? Breaking it out[109] *(continued)*

Target	Critical component	Measure of effectiveness	Potential asymmetric approach
Government services infrastructure	■ Capabilities at Federal, state, and local levels to coordinate essential needs of public	■ Federal, state, and local capabilities are able to effectively deal with emergency situations ■ Public faith in government services remains high	■ Physical attack using WMD or traditional terrorist means ■ IW attack aimed at disruption of operating systems ■ Overstress capability to respond by the scope of the potential event
Defense infrastructure	■ Military installations ■ Military units ■ Military command and control capabilities	■ Military installations, units, and personnel are able to execute missions without serious disruption ■ Public faith in military remains high	■ Physical attack using WMD or traditional terrorist means ■ IW attack aimed at disruption of operating systems
Population	■ Physical security ■ Well-being	■ No mass casualty attacks exceed the ability of appropriate government services to respond ■ The American people's sense of well-being remains high, including faith in American institutions ■ Effective counters are immediately employed against population attacks	■ Physical attack using WMD or traditional terrorist means ■ Indirect attacks against sense of well-being by successful attacks against supporting infrastructures ■ Multiple attacks that cannot be stopped

Examining Potential Vulnerabilities

Table 7 lists the ten categories of targets in the leftmost column. The second column identifies the critical components of each infrastructure—the nuts and bolts that must interact efficiently. The third column identifies broad measures of effectiveness that seek to establish how well the system must function in order to remain effective. While these measures of effectiveness are subjective judgments, they are conservative and reflect mainstream thinking on what a reasonable level of friction is

within the infrastructure in question. When considering the population, it becomes a more difficult task, since there is little empirical evidence on how the American people would react to direct attacks. Ineffective governmental responses and sustained successful attacks over time may have a greater negative effect than a single spectacular attack.

The last column identifies some asymmetric approaches that an opponent might use to attack infrastructures and the civil population.

The table shows, first, that while all infrastructures are vulnerable to both traditional and WMD attack, the common theme is their vulnerability to information warfare attacks. Information technology in the United States (and everywhere else in the developed world, for that matter) is characterized by a profound and overarching interdependence between systems.

A second theme is that, when considering attacks on the homeland, certain forms and methods of attack will tend to produce enormous leverage in the public mind: the use of WMD and massive information disruption are the most obvious. Other forms of attack, while capable of great local lethality, will not enjoy the same leverage.

Ultimately, the most important resource that must be protected is the population itself. All of the infrastructures directly contribute to this end, but the heart of the matter remains the requirement to protect Americans from harm. It is likely that American citizens will understand and cope with nonrepetitive attacks on our population and its supporting infrastructures. The most dangerous threat may be that of repeated, sustained attacks against the population or an identifiable infrastructure that the civil government is unable to stop. This is a tried and true recipe for terrorists through the years. When coupled with the capacity to generate mass catastrophes, it may prove to be the threat that we must guard against most strenuously.

Chapter Four

Categorizing the Threats

What rough beast, its hour come round at last, Slouches toward Bethlehem to be born?

—William Butler Yeats, *The Second Coming*

The previous two chapters have established the *what, who,* and *when* of asymmetry, and have also attempted to describe the military and civil structures and military operational practices of the United States that are the potential target sets for asymmetric actors. This chapter will integrate these two lines of argument, and attempt to make some clear distinctions about what the most dangerous threats are to the United States. This will form the basis for the policy component of this paper, chapter five, which will outline specific actions that can be taken to preserve both our military superiority and the integrity of the United States homeland from asymmetric attack.

It is essential to discriminate between different levels of threat. Otherwise, we are confronted by a veritable smorgasbord of threats—some reasonable, some incredible, but all difficult to plan for unless we differentiate between them. Thinking in a discriminate manner will lend structure and a comparative approach to asymmetric threats, and pay heed to the cautionary that "we should not spend more time inventing asymmetric options for other states than those states' leaderships do themselves."[110] At the same time, it is not productive, within the limits of this study, to establish a threat list that explicitly proposes, for example, a number 1 threat to the United States that is markedly different from a number 4 threat. It *is* productive, though, to posit that some threats stand out as more dangerous than others, and are therefore worthy of specific policy counters.

This selection of threats is based on the recurring themes that have guided the discussion of asymmetric warfare throughout this paper:

- Asymmetric actors pit strength against vulnerability, seeking disproportionate effect
- A perceived or actual disparity of interest is the enduring background to asymmetric approaches (and there is a crossover point that may prove deadly to the asymmetric actor)
- The target is the will of the opponent (and this is the psychological component of asymmetry)
- The desired effect is on the strategic level, regardless of the level of war the approach is implemented
- There is an interaction of threat and response that is based on what the United States does, as well as the culture of the potential asymmetric actor
- Effectiveness is important.

From this broad integration of the relative danger of each potential asymmetric approach against the potential targets, it is possible to extract the more specific set of dangerous threats that we will face. As a result of this, ten potential asymmetric threats are discussed below. They are not ranked, and none is singled out as "most dangerous" to the United States. Such a comparison would be invidious: these are all dangerous threats, and they are representative of other threats that have not been included. These ten threats form a reasonable spectrum of potential asymmetric approaches that could be practiced against the United States from which our own policy decisions can be crafted. Selection of these threats will allow detailed examination of potential scenarios, and it will also provide a more explicit basis for developing effective counters. "Future case studies" have been appended to some of the threats to provide a sense of immediacy.

What Are the Ten Asymmetric Threats?

The first asymmetric approach considered is *the threat of a nuclear or biological attack against the American homeland.* The damage that could be done by such an attack is much greater than any other possibility. For this reason, possession of nuclear or biological weapons and means of delivery give a regional competitor or a rogue state a credible means of influencing U.S. decisionmakers. This is true disproportionate effect. Any U.S. president would have to weigh alternatives of war and peace very solemnly against the U.S. national interest when the opponent

possesses the credible capability to deliver a nuclear or biological countervalue attack on the United States.

It is conceivable under certain circumstances (i.e., when a national interest of the United States is not unambiguously involved) that this type of threat would severely compress our range of options.[111] This is a threat that operates almost purely at the strategic level of war. As a threat, this is both a highly dangerous possibility and one that is increasingly likely, and for these reasons this alternative is the only asymmetric approach considered among these ten that is based on the principle of coercion and might not actually employ a weapon. It is the *threat* of attack that coerces or deters potential U.S. action in this case; an actual attack may well surrender many of the advantages of an asymmetric approach.

The threat of such an attack could include either covert or conventional means. Conventional means—cruise or ballistic missile, or manned aircraft—is less likely as a means of delivery for a non-peer competitor. Technological considerations alone would make it difficult to deliver such a weapon to the continental United States, and the trail back to the source would be clear and unequivocal. An alternative option would involve the covert infiltration of a nuclear weapon or a biological weapon into a major urban center. The possibility of an irrational state actor cannot be discounted, however, when the stakes are so very high, and the delivery of a small number of nuclear weapons by ballistic missiles should be considered a viable, though less likely "lesser included" case of this threat.

Crossing the line between coercion and actual attack would be a very dangerous step for any state. For this reason, coercive asymmetric approaches of this nature could be coupled with an intensive diplomatic and information operations campaign designed to achieve limited results below the threshold of actual use. The vignette that follows describes just such an attempt.

Vignette 1: The Disputed Middle Ground

Westland and Eastland share a common border and have been locked in periodic conflict going back generations over a disputed oil-rich area of several hundred square miles that lies between them. The area is controlled by Eastland. Eastland's oil is not considered vital to the United States, but it is vital to a number of Western European nations and Japan.

Westland is larger and more powerful than Eastland. Westland, because of its repressive governmental policies and attempts to foment revolution among neighboring states, is a regional pariah, but does enjoy some

level of support from states and nonstate entities, both in an out of the region, that are opposed to U.S. policies. Westland is largely equipped with legacy Warsaw Pact equipment, most of it in need of maintenance. Recognizing this, and having access to significant oil revenues, Westland has pursued many attempts to develop not only an indigenous WMD capability, to include biological agents and delivery systems, but also sophisticated delivery systems. They have tested the TRIGON–4, a ballistic missile with near-intercontinental range. It has been the best judgment of the CIA that Westland does not possess weaponized nuclear devices.

While Eastland does not have a formal defense treaty relationship with the United States, since the end of the Cold War it has purchased significant amounts of military equipment from the United States. Despite this, it is widely recognized that Eastland's military strength is only a fraction of Westland's, and in a general war between the two states, Westland will likely prevail. An informal relationship has been established between the United States and Eastland that includes periodic ground, air, and sea exercises of United States forces, partial prepositioning of selected military equipment, and extensive staff talks. Plans have been developed and refined for the rapid movement of air, ground, and naval forces to the defense of Eastland in the event of an attack by Westland. America's regional allies and NATO are full partners in these plans.

The discovery of new and extensive oil deposits in the disputed area breaks the uneasy peace between Eastland and Westland. Westland delivers a demarche *to Eastland demanding full control of the oil fields. Apparently, Westland has decided that its own oil fields, while still productive, are nearing exhaustion. Eastland's new fields offer the best hope for long-term economic security. Concurrently, Westland masses three armored divisions on the border between the two countries. It is the judgment of the U.S. theater CINC that these forces can overrun the disputed oil fields in less than 12 hours, and defeat Eastland within 72 hours, to include the occupation of the capital city.*

Eastland refuses the Westland demarche *and mobilizes the Imperial Guard. At the same time, Eastland secretly requests the deployment of U.S. forces. The regional commander-in-chief concurs, and requests the immediate movement of four AEFs, two Marine prepositioning brigades, two Army prepositioning brigades, and three carrier battle groups. While the Joint Staff is considering these requests, Westland fires what is assessed to be a TRIGON–5 missile that places a satellite on low earth orbit—a feat they were not believed to be capable of for at least another five years. A rapid*

CIA assessment of the missile's characteristics indicates that it could be capable of delivering a nuclear warhead-equivalent against more than half the continental United States, with a probable circular error of between five and ten miles.

Within hours of the successful launch of the satellite, a secret diplomatic communique from the "Maximum Leader" of Westland to the U.S. President is delivered through a third party's embassy. The note is short and to the point:

> We now possess 10 TRIGON–5 missiles. As you can see, they are capable of reaching your country. More to the point, we also possess a number of nuclear weapons, which we have obtained from former Soviet stocks. Photographs, weapons serial numbers, and other technical data on 10 of these weapons are appended. These weapons are in the 170-kiloton range. We invite you to double check this information with the Russians, who are unaware of these missing weapons. Additionally, we possess biological weapons that we have developed ourselves. You will also know that the TRIGON–5 possesses the throw-weight to carry these weapons to the United States, although regrettably our accuracy at this time will preclude their use against anything other than a large urban area. You will also note that the TRIGON–5 is capable of placing these weapons on orbit, and in such a manner that will invite exoatmospheric electromagnetic attack. Your scientists can instruct you in the potential effects of such a "nonlethal"attack.
>
> Our requirement is simple: we want co-ownership of the disputed oilfield. We do not demand the surrender of Eastland, and we do not demand Eastland's embarrassment—merely that Eastland recognize that Westland owns 50 percent of the oilfield, and that Westland will be the executive agent for the operation of the field. How you convince Eastland to accept this is your business. There can be no deployment of any U.S. air, ground, or sea forces into Eastland, or within 500 nautical miles of either the Eastland or Westland coast. Again, how you couch this in palatable terms to your regional and NATO allies is your business. We will not make political capital of your efforts here—so long as you do it.
>
> Last—doubtless your military leaders will argue for preemption of some kind. We urge you not to accede to this. Ask them how they did in "the great SCUD hunt" against Iraq—and know

> that should you undertake any military operation into Westland, two things will happen: we will detonate a nuclear weapon in conjunction with your attack on the outskirts of a major city in Westland and then blame you loudly and effectively; second, we will destroy a major American urban area. Alternatively, we may select an exoatmospheric HEMP attack. And, of course, you cannot be certain that the satellite now on orbit does not carry a radio-command nuclear weapon. As you know, it crosses over the United States many times every day. Ask your scientists what the effects will be of a 170-kiloton low-earth-orbit explosion. In closing, we ask you to consider whether these oil fields really constitute a vital national interest to the United States, particularly when we are more than willing to cooperate with you in concealing the fact that this dialogue—and our new capability—ever existed. This is a matter of national survival for us. Is it a matter worth the lives of millions of American citizens?

The next asymmetric threat is that of *a concerted information warfare attack against our national information systems infrastructure,* to include the information management systems vital for the operation of the critical infrastructures of public safety, transportation, and banking and finance. The relative likelihood of this attack is high, given our dependence upon such systems. The potential damage could be severe, but it would probably not approach the devastation possible from a nuclear or biological attack. The single caveat to this assessment would be that a HEMP strategic attack on the United States could be devastating to the entire national information infrastructure. Because of the combination of opportunity and vulnerability, this is assessed as a very real threat, whose potential scope will only grow with time.

Such an attack targets the will of the United States by operating directly against the civil population. It enjoys disproportionate effect, and, if used as a threat or coercing tactic, could have many of the deterring advantages of nuclear and biological weapons.

Such an attack could run the gamut from attacks of precision disruption aimed at specific elements of infrastructure (air traffic control systems, for example) to a culturally disruptive attack based on HEMP.[112] The United Sates remains uniquely vulnerable to these forms of attack because of the increasing digitization of virtually everything in both the public and private sector.[113] In fact, the complete interdependence and system of systems approach that characterize information

technology make it very difficult to predict the top end scope of a successful IW attack.

What is clear, though, is that a HEMP attack would be profoundly destructive to the American way of life. As already discussed, a nuclear weapon detonated at between 100 and 500 kilometers above the center of the country would cause no deaths due to direct effects (fire, blast, radiation), but could cause thousands of deaths due to the creation of an adverse electromagnetic environment: massive power loss, aircraft flight control systems failures, the possible destruction of the commercial satellite constellation, and a myriad of other effects that would, in all likelihood, have the ultimate effect of ending, at least temporarily, the information age in this country.

The dangers to the attacker are very high in a strategic HEMP attack. As has already been outlined, the strategic command and control and continuity of government functions of the United States are protected against this type of attack, and the track of a missile or a weapon already on orbit would be easy to investigate. It would be much more difficult to find the responsible party involved in a less direct information warfare attack. As proposed below, such an attack would gain effectiveness if employed in concert with other asymmetric operations. In the vignette below, and continuing the argument of vignette 1, Westland elects to conduct a biological attack on the United States and follow it up with a cyberattack that will take advantage of the additional stress placed upon power and other systems.

Vignette 2: Cyberattack on New York—A Matter of Trust

It is rush hour in New York City. At the very busy 34th Street Subway Station of the Red Line, no one notices two small light bulb-size glass containers that are thrown onto the track. Each contains ten grams of weaponized bacillus anthracis. *Within minutes, 20 grams of dried anthrax spores are circulating among the commuters on the crowded Red Line. Theoretically, one gram of dried anthrax spores contains approximately 10 million lethal doses.*[114] *Within 2 or 3 days, hospitals throughout the New York area are reporting large numbers of people with fever, malaise, and other flu-like symptoms. Within 4 to 5 days, it is clear that this is not the flu. Although some people improve for short periods of time, respiratory distress sets in rapidly, along with a host of other life-threatening symptoms. Medical intervention generally cannot reverse the course of the disease after the onset of symptoms, and so the vast majority of people who are sick will die.*

If 1 percent of the population of New York City were infected—about 126,000 people—then fatalities would number around 120,000. The high number of fatalities reflects the simple fact that after the onset of clear symptoms, treatment is usually ineffective. Probably another 1.3 million people would flood the already overloaded medical system—the "worried well," who are uninfected but frightened. The emergency services systems within the New York area would be overwhelmed.

By the third day of the anthrax attack on New York City, the hospitals in Manhattan and in the adjoining boroughs are overwhelmed; the National Guard has been called out and federalized, and the U.S. military is beginning to deploy medical and other support elements into the city. Just after dark along the east coast of the United States, hackers operating from outside our borders gain access to the protected servers of Consolidated Edison. They are helped in this by a well-paid insider, who furnishes them with the access codes needed to gain system administration privileges. Consolidated Edison buys most of its power from Canadian sources, and the electrical grid is controlled through an Oracle-based operating system and database. The system used by Consolidated Edison, unlike Oracle software used by the U.S. military, does not use "trusted software." Elements of the code have been written outside the United States. This allows the insertion of malicious code into the system that was dormant until called to life.

Within two hours, most of New York is without power. A chaotic situation becomes disastrous on Manhattan. But, within six hours, the damage to the automated power management grid has been repaired, and as the sun comes up the next morning, power has been generally restored—but hundreds have died throughout the night, particularly patients who were on respirator support—a characteristic of anthrax therapy—in overflow annexes to New York's hospitals. Military power systems are unaffected, and most hospitals are able to run off their own internal generators, but many of the patients are not in the hospitals. In isolation, this would not have been a particularly damaging attack, but when executed in concert with other measures, it provokes a powerful and lethal synergy.

The next asymmetric threat is that of *biological and chemical attacks against host nation support and alliance forces in an area of responsibility,* with the dual goal of splitting a coalition and eroding the national will in the United States. An attack of this nature would seek to exploit weaker elements of a coalition by attacking with principally biological and chemical weapons. The relative likelihood of this form of attack is high in a major theater war environment, and the relative danger to U.S.

and allied forces is high. Because of its potential effectiveness, the threat of this form of attack could also be used to coerce potential regional allies in the early days of a crisis.

Such an attack—or threat of an attack—would be directed against the weakest elements of any coalition or host nation. It would strictly avoid targeting U.S. forces, and would instead be directed against the personnel who are the vital theater enablers for U.S. forces. The most lucrative form of this attack might be to target civilians critical to offloading U.S. equipment as it enters a theater. They will not be under military discipline, will not have any NBC training and will have little or no protective equipment, to include the requisite series of inoculations that U.S. and allied forces presumably will have had. These workers are the Achilles' heel of any theater that will require the heavy flow of U.S. forces through a limited number of ports of entry, either air or sea.

If the will of regional allies can be degraded by these threats or by actual employment, then it could have a pernicious effect on the will of the United States to participate. For a regional aggressor, it follows that threats would initiate eventual use. It might be that good effect for the aggressor could be obtained by simple coercion, but the line from threat to employment is easier to cross within a regional scenario, and when the primary targets will not be U.S. forces.

Vignette 3: Just Getting There!

It is C+3 in a major theater war. Southland has been invaded by its hostile neighbor, Northland. The United States has begun execution of a longstanding contingency plan to flow forces into the two deepwater ports and three international airfields in Southland. The U.S. plan calls for the rapid introduction of theater airpower to slow the advance of the four mechanized and two infantry divisions of Northland, and then the movement of U.S. ground forces by strategic airlift to link up with two prepositioned brigade sets of equipment, and two prepositioning brigade sets that will arrive by fast sealift by C+5. During the morning of C+3, though, symptoms of anthrax are noted in small numbers of stevedores who will work to offload the ships as they arrive. The numbers affected are small, but simultaneously Northland begins to broadcast this to the entire world via CNN and the internet. Within 24 hours the ports are virtual ghost towns, as the workers flee the urban centers. The United States offers inoculation to its Southland allies, and feverishly works to vaccinate all members of the international coalition, but there isn't enough vaccine. U.S. civil reserve pilots decline to fly to destinations in the theater that have reported infection. The

panic factor dramatically increases the reporting of both real and imagined cases of sickness, and allied nations within the AOR close their borders to U.S. deploying forces. The effect of this is to slow the ability of U.S. airpower to maintain the sortie generation rate required to slow the Northland attack. Southland, seeing this and realizing that U.S. ground forces will not be arriving in a timely manner, elects to sue for peace and cedes large portions of its nation to Northland.

The next asymmetric threat is that of *WMD attacks against strategic deployment systems*, including air and seaports of debarkation in theater, en route facilities, and enabling infrastructure. The primary threat is that of chemical and biological weapons. The relative likelihood of an attack such as this is high in a major theater war or near-major theater war scenario. The potential for damage is high. Many of the considerations that apply to the previous threat, attacks on allied and coalition forces, are also operative here. There are also some greater risks, because in this case the attack is now being delivered directly against U.S. forces as they enter a theater.

An attack of this nature would be a central component to an antiaccess strategy that would seek to slow the arrival of U.S. forces into an AOR. Chemical attacks would be the least effective but easiest to execute. Biological warfare attacks would gain high leverage—it would not take more than a very small attack, coupled with an aggressive information operations plan, to severely disrupt the large number of nonmilitary enabling systems that support the deployment architecture. It is possible that a lesser included or alternative to this form of attack would be the aggressive employment of *conventional SOF* and perhaps terrorists who operate against the deployment infrastructure without using WMD.

Vignette 4: Just Getting There—Again

It is C+3 in a major theater war. Southland has been invaded by its hostile neighbor, Northland. The United States has begun execution of a long-standing contingency plan to flow forces into the two deepwater ports and three international airfields in Southland. The U.S. plan calls for the rapid introduction of theater airpower to slow the advance of the four mechanized and two infantry divisions of Northland, and then the movement of U.S. ground forces by strategic airlift to link up with two prepositioned brigade sets of equipment and two prepositioning brigade sets that will arrive by fast sealift by C+5. Concurrent with its attack south, Northland unleashes a barrage of improved SCUD–B missiles on the arrival ports and airfields that U.S.

forces will use, and the operational airfields that U.S. airpower is operating from. Their warheads contain VX, and while the accuracy isn't particularly effective, large areas of the ports and airfields are blanketed with the persistent agent. The immature theater ballistic missile defense system proves effective against only about 60 percent of the incoming missiles, and Northland is believed to have a SCUD–B stockpile of several hundred. This has two immediate effects: The deployment of U.S. forces is significantly slowed, and large elements of U.S. airpower must be dedicated to "SCUD-busting," which brings a poor return on the investment in time, pilots, and aircraft. The result is that Northland forces are able to overrun most of Southland before the U.S. deployment can be completed, and U.S. forces are withdrawn to neighboring countries—and subsequently face the need to execute a forcible entry operation in order to restore the territorial integrity of Southland.

The next asymmetric threat is that of *information warfare, including the threat of HEMP attack against forces in an AOR.* This is a potent threat across the spectrum of information operations, but the most dangerous form is the use of HEMP to degrade U.S. and allied capability to achieve information dominance. The relative likelihood of this form of attack is moderate—the technical requirements to successfully prosecute such an attack are daunting—but the danger to U.S. forces would be very high if the attack proved successful.

As a general principle, offensive information warfare will grow less fruitful for an opponent as the level of warfare moves from strategic to tactical. It is harder to enter U.S. tactical computing systems, and a variety of aggressive U.S. defensive information operations will be concurrently taking place. The use of HEMP at this level, though, maximizes the advantages of disruption inherent to this weapon while minimizing the dangers of an attack on or above U.S. soil with nuclear weapons.A HEMP attack in a regional conflict would strike directly at the heart of the U.S. concept of warfighting: the rapid management of information. It might be possible to destroy all tactical communications in an AOR, severely degrade theater communications, destroy all satellite support functions, damage or destroy many aircraft, and cause a staggering number of potential problems in virtually all U.S. military equipment.

States that possess nuclear weapons and delivery systems will also have the potential deterring benefit that accrues from this capability. In actual operation, however, this threat would exist below the strategic level, although favorable strategic effects could be secured by operations that follow such an attack.

Vignette 5: Fade to Black

It is C+10 in a major theater war. Southland has been invaded by its hostile neighbor, Northland. The United States has executed a longstanding contingency plan and has deployed forces into the two deepwater ports and three international airfields in Southland. U.S. airpower has stopped the advance of the four mechanized and two infantry divisions of Northland, and U.S. ground forces have linked up with two prepositioned brigade sets and two prepositioning brigade sets, and have begun to establish themselves in the field. Southland forces have defended in good order and are ready to undertake offensive operations. The theater commander is preparing to counterattack to restore the international boundary between Southland and Northland. Just after midnight on C+10, Northland fires a modified SCUD to a high altitude over the battlespace. While SCUD firings are not new in this theater, the assessed trajectory does not fit an attack profile that has been experienced before. The theater staff is still in an attack assessment conference with SPACECOM when a 100-kiloton nuclear weapon detonates at an altitude of 200 kilometers near the geographic dead center of the battlespace.

A number of things happen very quickly on the ground. Tactical communications cease; vehicles with advanced solid-state electronics stop running. Many theater backbone data transmission up- and down-links are rendered useless. In the air, Army helicopters literally fall from the sky, and some Air Force aircraft are brought down as well. The JSTARS picture disappears, and no contact can be established with the aircraft; the same is true for AWACs.

On the beach, U.S. Navy ships can be seen on the horizon, but it isn't possible to communicate with them electronically in the hours after the explosion: much of their electronics have been damaged as well.

The worst damage, though, is reserved for space-based systems. The effect of the explosion charges the Van Allen radiation belt and destroys all commercial satellites in low earth orbit (LEO); satellites in half-geosynchronous and synchronous orbit, including GPS satellites, have varying degrees of adverse effects. While assured command and control systems based on MILSTAR remain active, virtually all other satellite communications systems cease to function, either immediately, or in the near future.[115] *The CINC has lost his common operating picture.*

No American troops are killed or injured as a result of the explosion itself. In fact, it will eventually be determined that the explosion occurred over Northland.

As the dark sun fades, the theater commander realizes that instead of fighting with the principles of JV 2010, *he must now face Northland with tools and techniques that would be well known to Sir Douglas Haig in front of Passchaendale in 1917. The core principle of U.S. warfighting doctrine—the ability to rapidly and efficiently share vast amounts of information—is no more. On this new battlefield, high-lethality systems will now fight with very limited intelligence beyond direct visual range.*

Northland formations continue to move south. They appear to have suffered degradation as well, but they now enjoy an uncontested numerical superiority in what is becoming an infantry fight.

The next asymmetric threat is that of *battlespace selection*: we may be forced to fight in places where our information and other forms of superiority are blunted. A scenario such as this would see an opponent seeking to lengthen our operations in time while maximizing opportunities for U.S. casualties. The relative likelihood of this method of attack is high—if the terrain will support it—and the potential for danger is also high.

The world is becoming more urbanized,and U.S. forces will often be forced to enter and operate in this terrain—perhaps most of the time. The examples of Stalingrad, Hue City, Manila, and Mogadishu are clear and evident.

Vignette 6: Going to Town—Terrain and Warrior Tactics

Northland attacks Southland with little warning. Due to unfortunate geography, the Southland capital, Prime City, is located just 40 kilometers from the international border between the two countries. Within 24 hours, the Northland strategy is clear: attack to seize Prime City with a combination of infantry and SOF, while mechanized formations fan out in an attempt to bypass the city. By the very speed of their attack, they are able to overrun the suburbs of Prime City, which has over 12,000,000 occupants, spread over several hundred square miles of developed terrain. By use of SCUD–Bs with chemical warheads fired in persistent barriers, they have prevented the population of Prime City from fleeing south; instead, they remain largely within the city, and are now subject to the vicious street-to-street fighting that is going on between Northland attackers and Southland defenders. U.S. forces, some already within Southland, respond immediately. The CINC has long argued with the Southland General Staff that Prime City should not be defended; it is too close to the border, and the huge urban sprawl makes it very hard to employ sophisticated U.S. sensors and weapons. Now, in the heat of battle, and with the city's population still trapped within,

Southland leaders make it clear that they plan to fight the decisive battle of the war in Prime City. In the open areas away from Prime City, much of Northland armor has been destroyed or has gone to ground to avoid U.S. airpower, but the battle still rages within the capital.

By C+7, there are three divisions of Northland infantry in Prime City, and they hold a little less than half of its area. The CINC's preference would be to methodically isolate the city from Northland lines of communication, and then let Northland forces starve. The fact that there are over 10,000,000 civilians still within the city, though, makes this strategy untenable. On C+8, there are video reports from within the city of mass executions, and it becomes clear that it will be Northland strategy to force the U.S. military to enter the city and fight to retake it: the alternative will be to stand by while millions of innocent civilians are killed. The pressure from Southland on the U.S. NCA is strong, and on C+9, U.S. infantry begin to fight their way into the city. It will be a long and bloody process, even with abundant close air support and the latest in urban warfighting technology.

The next asymmetric threat is that of *non-WMD antiaccess measures,* namely, mines, missiles, and other tried-and-true measures that can slow deployment or forcible entry operations. The relative likelihood of these tactics being employed is high, and the potential for damage at the operational level is also high.

This approach applies legacy systems from the Cold War along with newly emerging systems to prevent the entry of either amphibious, airborne, or air forces. It is a tactic that has limited opportunity for success unless applied in concert with other measures. This has the greatest chance of success in a small-scale contingency, where there is no direct U.S. vital national interest at stake. The Serbian air defense system during *Allied Force,* already discussed, is an excellent example of just such an antiaccess strategy.

The next asymmetric threat is that of the employment of *warrior tactics*; methods of fighting and conduct on the battlefield and in a region that grossly violate norms of behavior in an attempt to shock and disrupt an opponent. The relative likelihood of these tactics being employed is high, and the potential for damage to U.S. forces is moderate. Vignette 6 incorporates an example of this approach.

Another asymmetric threat is that of a *chemical attack against the continental United States*. The potential for chemical attack is often left in the shadow of the biological warfare threat to the homeland, but it is a distinctly separate threat, with a slightly higher relative likelihood of

being employed. It is more likely because it is easier to introduce chemical weapons into the United States than nuclear weapons. This is also a less dangerous method of attack, for it does not draw the international revulsion that attends biological weapons. The potential for large-scale damage to the United States is low. This is less an alternative for state actors than for nonstate actors with limited resources and delivery alternatives.

The last asymmetric threat is the one that we can't even envision: *the wild card*. Threats will emerge that we cannot plan for. While most of them will spin off what the United States does, they will take root in the fertile soil of their own unique culture and basis of experience, and may prove to be the most dangerous of all.

Table 8 summarizes our assessment of what constitutes the ten asymmetric threats to the United States worthy of consideration. It is important to reemphasize that this is certainly not intended to be an all-inclusive list of threats. Other threats that are both lethal and dangerous

Table 8. Summary of ten asymmetric threats

Threat	Relative danger	Relative likelihood
Threat of nuclear or biological attack against the U.S. homeland	High	High
Information warfare (IW) attack against U.S. homeland*	Moderate	High
Biological and chemical attacks against host nation support and alliance forces in an area of responsibility (AOR) (coalition splitting)	High	High
Weapons of mass destruction (WMD) attack against strategic deployment systems	High	High
IW (including high-altitude electromagnetic pulse) attack against forces in an AOR	High	Moderate
Battlespace selection	High	High
Non-WMD antiaccess measures	Moderate	High
Warrior tactics	Moderate	High
Chemical attack against U.S. homeland	Low	Moderate
The Wild Card	Unknown but potentially high	High

** An electromagnetic pulse attack would raise the relative danger to "High" in this category.*

have been omitted for various reasons. For example, a direct WMD attack against U.S. forces is not included here, based on the judgment that such a nuclear attack (however effective) would surrender many of the advantages of asymmetry; and chemical and biological attacks against fielded U.S. forces, while certainly dangerous, will not dramatically change the outcome of an engagement. In the area of information operations, the cyber and EMP threats are emphasized, even though traditional information warfare techniques remain a very real and dangerous threat.

Conclusions

Four of these threats employ some form of WMD as their principal operative element. Two of the threats explicitly employ information operations, while several others would depend heavily upon information operations as a supporting element of the primary strategy. Two are relatively "low tech" approaches.

The WMD approaches all have a significant deterring component, and actually draw their strength from the disproportionality inherent in possession of nuclear or biological weapons. This approach, and, to a lesser degree, the others, seek to cause the United States to be very cautious about what will be declared a vital national interest. There is, however, a flip side: much of the disproportionality and all of the advantages of disparity of interest would be lost in the event of an actual employment of these weapons.

Based on this understanding of what the main asymmetric threats to the United States are, what actions can be taken to counter them? This will form the basis for the next chapter.

Chapter Five

An Option of Difficulties—Countering Asymmetric Threats

In 1759, British General James Wolfe, in examining the redoubtable French fortress of Quebec, observed that "war is an option of difficulties." His words ring as true now as then. Nothing is ever easy in war, or in planning for war. Remembering this is a good starting point for the final part of this analysis, because when examining actions we can take to counter asymmetric threats, none will be easy, and we will often have to choose from a range of difficult choices.

This chapter begins by outlining what steps are being taken now to reduce the dangers of the asymmetric threats to the United States identified in chapter four. A short summary of existing programs and policies that pertain to each threat will be introduced. Any recommendations for a way ahead must have a sound grounding in current practices. In many of these areas, it will be argued that we can and must do better. It will be proposed that the starting point for improving our responses is the establishment of a broad conceptual model to counter asymmetric threats that will provide a framework for specific responses. Three concepts for dealing with asymmetric threats will be introduced. Linked to each of these three main ideas will be a series of specific policy recommendations that address deficiencies in current approaches. Some of these recommendations encompass a broader arena than the Department of Defense. The chapter will close by looking at the potential programmatic and political costs of implementing these recommendations.

Current Initiatives: The State of Play Today

In the area of *the threat of nuclear or biological attack against the U.S. homeland,*[116] six principal policy initiatives are active:

- Maintenance of a credible policy of not ruling out use of nuclear weapons in response to WMD employment against the U.S. homeland, U.S. forces, or allies

- Continuing implementation of PDD–62 (Combating Terrorism)[117]
- Continuing implementation of PDD–39 (U.S. Policy on Combating Terrorism)[118]
- Implementation of the Defense Against Weapons of Mass Destruction Act of 1996 (Nunn-Lugar-Domenici amendment to the National Defense Authorization Act for 1997)[119]
- Implementation of provisions of PDD–63 (Critical Infrastructure Protection)[120]
- Continuing to conduct tests in advance of a decision on fielding an effective limited national missile defense system capable of high-confidence interception of small numbers of ICBMs.

The United States has no capability to defend the homeland against *ballistic missile-delivered WMD attack*. The success or failure of a ballistic missile attack would depend solely on the technical competency of the attacker. Any asymmetric actor can see the advantages of developing some form of this capability.

Of course, a ballistic missile-delivered attack is only one of many options open to an opponent seeking ways to attack the U.S. homeland with WMD. Covert delivery may be more likely.[121] A broad variety of initiatives are underway at the federal, state, and local levels to prevent or minimize the effects of a biological or chemical attack. Despite these encouraging developments, many of these initiatives are still immature, funding is inadequate, and much remains to be done in the area of consequence management in terms of training, organizing, and health system enhancements. There is little agreement on who is in charge, and little rationalization of federal, state, and local organizational arrangements. Metrics need to be established to determine investment and training requirements.[122]

In the area of an *information warfare attack against the U.S. homeland*, there are two principal active initiatives:

- Implementation of the recommendations and provisions contained in the Report of the President's Commission on Critical Infrastructure Protection as embodied in PDD–63
- Establishment of Joint Task Force on Computer Network Defense (JTF–CND).[123]

The scope of the information warfare problem is now well understood, and within the Department of Defense an aggressive program is underway to remedy known deficiencies. The potential problem is more difficult in the private sector, where myriad opportunities for attack must be

balanced against the robustness and diversity of the communications infrastructure itself. The United States remains singularly vulnerable, particularly in the private sector, to potential HEMP attack. The more complex and the more interdependent a system is, the more vulnerable it becomes.

In the area of a *WMD attack against strategic deployment systems,* two initiatives are active:

- Conducting tests and moving to field an effective theater ballistic missile defense (TMD) system
- Limited tactical decontamination systems at APODs, SPODs, and other organic unit capabilities are being fielded.[124]

The United States currently has only a very rudimentary and limited theater-level ballistic missile defense system, although extensive investments have been made in both land- and sea-based systems. The decontamination and detection systems now fielded would be stressed to provide coverage for U.S. personnel, and will certainly be inadequate to protect HNS personnel vital to the theater deployment infrastructure.

In the area of *information warfare (including HEMP) attack against forces in an AOR,* limited initiatives are underway. Initiatives in this field are generally related to protection of information systems from cyberattack. Limited actions have been taken against the HEMP threat.

This area is a key vulnerability. Significant changes are needed now in existing policy on HEMP protection. Existing standards do not cover all military systems, and even more civilian systems are unprotected. The increasing emphasis on commercial off-the-shelf (COTS) systems for military application only increases the potential danger. Coalition interoperability requirements may also raise additional challenges to system integrity and protection.

In the area of *biological and chemical attacks against HNS and alliance forces in an AOR (coalition splitting),* while U.S. forces possess varying degrees of chemical and biological protection, our potential allies and coalition partners, particularly those outside of NATO, are trained and equipped at a much lower level. Additionally, in a regional war scenario, the civilian populations of potential allies and host nations will be directly vulnerable to this form of attack.

In the area of *battlespace selection,* no clear solution is at hand. The services are pursuing their own visions of how to address this threat. The Army Dismounted Labs and the Marine Corps *Urban Warrior* series of experiments are dealing directly with these challenging issues. Joint Staff efforts during the last JSR/QDR cycle helped the joint community

focus on the problem. Joint doctrine efforts are proceeding. It is still too early to tell how effective the U.S. Joint Forces Command (JFCOM) initiatives will be in establishing a joint perspective. The challenge for an expanded JFCOM role in experimentation will be to preserve a healthy diversity of approach at the service level, while ensuring interoperability at the joint level. The jury is still out on how effective JFCOM will be in catching up on service efforts and achieving this delicate balance of oversight and nurturing.

In the area of *non-WMD antiaccess measures*, the same initiatives as stated above are active: service initiatives predominate, and there is little joint consensus, though there are signs of growing awareness.[125] The recently initiated JFCOM Joint Experimentation Programs may be useful. The Navy is working aggressively to address the mine warfare component of the problem, but much remains to be done.

Initiatives in the areas of *warrior tactics* and *wild card threats* share common themes: some innovative work is proceeding at the service level, but there is little at the joint level. The Joint Nonlethal Directorate is the principal exception to this. Aside from service-level experimentation, there are few attempts to explore the extent of what is possible. The Marine Corps Ellis Project and the Chief of Naval Operations Executive Panel are each examining the possibility of technological surprise. More thought needs to be given to studying and "red teaming" foreign military options, such as the translation of Chinese writing on military developments sponsored by the Office of Net Assessment within the Pentagon. Across the board, it seems likely that this effort will benefit from the greater focus and depth that JFCOM experimentation programs will bring, if properly implemented.

Summarizing Current Initiatives

The programs and policies selected as a starting point are representative, not all-inclusive. There undoubtedly are others that arguably deserve greater emphasis. Even bearing these considerations in mind, establishing an understanding of where our efforts are seems to be the natural starting point for determining where we can do better.

Two key observations can be drawn from this policy overview. First, broad disparities in level of effort, interest, and potential effectiveness mark our responses across the threat areas. This is related to the second key observation: no overarching or coherent theme ties all elements of potential asymmetric counter measures together. This lack of a unifying

theme follows from the differing definitions of asymmetry that have influenced policies. Improving our responses to the asymmetric threat must begin with adoption of a consistent philosophy of how to deal with asymmetry, based upon a consistent definition. Such a philosophy can be derived clearly and simply from the recurring themes of asymmetric approaches laid out in this study.

Doing Better: Beginning with Three Ideas

To effectively counter asymmetric threats, our policies need to reflect three interlinked concepts. First, our policies must *minimize our vulnerabilities to asymmetric attack* by deterring potential attackers and by having the capability to successfully defend against asymmetric attacks against both deployed forces and the homeland, if deterrence fails. Should an asymmetric attack prove successful, we need demonstrated competency in consequence management at home and the operational flexibility to prevail in the face of asymmetric attack for deployed forces. Possession of these capabilities will tend to make asymmetric attacks less attractive to potential adversaries.

Second, our policies must *accentuate our unique strengths* by continuing to pursue transformation objectives that embody the operational expression of *Joint Vision 2010* and its successor documents. In doing this, we must avoid overreacting to asymmetric threats. The American way of war, emphasizing speed, shock, and rapid battlespace dominance, is inherently asymmetric itself when compared to the capabilities of most potential opponents. Our way of war works, and we do not need to overcorrect in attempting to anticipate asymmetric approaches.

Third, in dealing with asymmetric threats, it will be critical to *prevent disproportionate effect*. This is the heart of asymmetric advantage, and it must be countered at all levels of war, although preventing the upward migration of tactical and operational effect to the strategic level is the most important component of this approach.

These three ideas all support what must become a basic understanding of the Department of Defense in dealing with asymmetric issues. For the United States, disparity of interest with a broad range of potential opponents is an enduring reality. As long as we remain a global power with many strategic interests, some interests will always be less important than others. It is the DOD operational task in dealing with the issue of asymmetric warfare to ensure that United States foreign policy options are not artificially circumscribed or compressed by state or nonstate actors who,

by threat or action, seek to impose a disproportionately high price on our engagement in an issue when it is inimical to their interests.

Policy Recommendations

A number of specific actions are recommended to implement this objective. In order to maintain coherence, the recommendations are grouped under the three organizing ideas: minimizing vulnerabilities, accentuating our unique strengths, and preventing disproportionate effect. Some of these recommendations will require broader action from departments and agencies across the Federal Government, as well as state and local governments. When a proposed action falls partially or wholly outside the Department of Defense, this is noted. There is significant overlap between the recommendations, and most will have positive effect under more than one organizing idea. Thus, these recommendations are not prioritized, nor are they listed in a proposed order of adoption.

Specific Actions to Minimize Vulnerabilities

We must act to reduce the direct threat of strategic attack against the American homeland. This requires the earliest possible deployment of an effective limited national missile defense system (NMD) capable of high-confidence interception of small numbers of ICBMs. This recommendation acts against the threat of direct attack on the United States homeland with ballistic missile-delivered WMD. It is understood that such a defense will only limit one potential avenue of attack for an aggressor, who may still choose to employ a myriad of covert means to attack the United States with WMD. It is also understood that deploying a ballistic missile system should only be part of a comprehensive approach to strategic defense. A comprehensive approach to this problem must also embrace a broad range of counterproliferation initiatives, an explicit deterrence strategy, and a variety of activities designed to prevent or minimize the possibility (and consequences—see recommendations that follow) of a covert attack.

Despite the fact that a ballistic missile defense system will only provide coverage against one of several attack options, it is still recommended, principally because it will complicate a potential attacker's problem by removing one offensive alternative.[126] The operative word in the statement of the problem is "threat." Defensive systems of this nature act explicitly to reduce a component of the potential threat, thus expanding the choices for future NCA when confronted with an opponent armed with WMD-equipped missiles.

We must also act to reduce the threat of direct or covert WMD attack on the homeland by demonstrating a capability for consequence management. This requires the expansion of the Nunn-Lugar "first responder" training from its current level of 120 cities to at least 240 cities as soon as possible. Larger cities may need larger teams, and perhaps more than one or two. A number of key supporting actions are recommended in concert with this proposal:

- The existing system for regional stockpiling of medical equipment and medicines, which is controlled by the Centers for Disease Control (CDC), should be expanded, based on updates from the intelligence community. This system should include methods for inventory control with "global visibility." The DOD should be tasked to develop contingency plans for rapid movement and concentration of these resources.
- Significant improvements have been made in the level of epidemiological monitoring within the United States; these efforts, also under the direction of the CDC, should be continued. This will be helpful in more rapidly detecting a covert biological or chemical attack.

We need to continuously reevaluate the basis for our planning. Current efforts have been criticized as being too rooted in the threat of "what people think terrorists *could do*, not on what they *have done* in the past or what they are *able to do* given considerable technical difficulties of procurement, production, and delivery."[127] This can lead to programmatic decisions that are too focused on "worst case planning, which may skew governmental focus away from the types of attacks that are more likely to occur."[128] All of our programs need a healthy sense of balance: there are too many scare scenarios out there now. This tension between worst case planning and a broader-based approach must be observed at all times. It isn't a bad thing, because it tends to cast a skeptical eye on the more outrageous possibilities. While the bioterrorism of *The Cobra Event* may make for chilling reading, in Oklahoma City a "conventional" attack was the deadliest terrorist incident ever on American soil.

In the long term, Department of Defense support for local and state agencies for consequence management (CM) should come primarily from the Reserve Components, and over time elements of the Army National Guard should be restructured to reflect this.[129] This can be accomplished by dual-missioning in the short term; ultimately, however, the requirement for WMD response and consequence management in the continental United States should evolve into a primary mission for the

Army National Guard. This is a natural choice because of the long affiliation which the Army National Guard has had with local governmental structures and its ultimate responsibility for the defense of the United States. When in a state supporting role, the Guard is exempt from the provisions of *posse comitatus* (18 USC 1385), which prohibit Federal military forces from performing law enforcement duties.[130]

Restructuring should be oriented toward enhancing and broadening the extant capability to assist in routine and contingency planning for CM activities and in incident response. Incident response would include C^4 infrastructure support, augmentation of physical security, emergency mobile medical assets, NBC reconnaissance, and mass evacuation operations if required.[131]

The capability to deploy from the United States for some of these forces will become of lower priority. Eventually, first call on designated elements of the National Guard force structure should be linked to requirements for WMD (and other) consequence management within the United States, and only secondarily any requirement to deploy on short notice in support of theater contingency plans. This will require a huge change in thinking on the part of the Guard—it will need to reorient inward as a first priority. There will be resistance to this idea, and it may be argued that such a reorientation of a significant portion of the National Guard will dissuade enlistments, particularly among potential soldiers who seek service in combat and combat support forces. While not minimizing this recruiting challenge, there is an obvious attraction of recruiting for forces that could make a concrete difference in six hours in a national emergency, rather than perhaps in 120 days in a "second major theater war (MTW)" CINC operations plan.

Under this proposal, the highest priority for the National Guard would be pre-attack, attack management, and post-attack consequence management within our borders. The National Guard would still retain the ability to support limited rotational deployments overseas in support of the active component, and would still have a "strategic reserve" mission, although it would no longer be explicitly linked to short-term regional warfighting operations plans. The restructuring of the Guard would be designed to increase the current numbers of low-density, high-demand units critical to consequence management: chemical, medical, military police, and other combat service support capabilities.[132]

The first step toward this end would be a detailed analysis of just what would be required to make such a broad change in thinking,

capabilities, and supporting structure. Such an analysis would of necessity encompass more than just the National Guard, because of the growing role of the Guard in rotational deployments in support of peace, humanitarian, and other operations. The increasing percentage of critical combat service support force structure embedded in the Reserve components will need to be closely reevaluated, although this proposal would not necessarily require large adjustments in this area. This is a good time to conduct such an analysis and to act on its findings. The comprehensive restructuring of the Army invites a parallel renaissance in the National Guard. These changes would reaffirm the long-standing relationship between the American people and the National Guard and return something directly to the communities with whom the Guard is affiliated.

Specific Actions to Accentuate Unique Strengths

We need to take immediate steps at the interagency level to improve our strategic intelligence posture that monitors the global environment and actively scouts for potential asymmetric approaches that might threaten us. This effort must go beyond our traditional adversaries and examine new and innovative threats that may arise. "Wild cards" will emerge, and the earlier that we can sense them, the more effective our response will be. In many cases, the knowledge that we are looking and listening will present a potential deterrent effect in and of itself.

This will require substantial retooling of our technological base for information collection as it listens to a world that is both increasingly encrypted and less dependent upon broadcast signal.[133] The qualitative edge that the United States enjoyed for so long in electronic monitoring has evaporated, and we may never be able to fully recover it. The expanded use of human intelligence will only begin to fill this void.[134]

A key element of intelligence gathering is ensuring it is ultimately disseminated to those who need it, both within the United States and among our allies. This is typically the greatest weakness of any intelligence program. Part of this practice of expanded dissemination must be the continuous process of sharing the latest available information on and counters to potential asymmetric threats with allies and likely coalition partners.

We need to take steps to assure that we will have continued access to those areas where we may be called upon to deploy in order to deter, and, if necessary, to fight and win. Specific components of this are:

- Field effective theater ballistic missile defense systems, both upper and lower tier, that will provide high-confidence coverage of arrival

airfields and ports, their associated assembly areas, airbases, critical host nation support infrastructure, and both U.S. and allied land- and seabased forces.[135] The current approach to testing and deployment appears to be broadly on track.

- Through military-to-military contacts with allies and potential coalition partners, ensure a common competency in NBC protection is established and maintained, and that procedures are established and rehearsed as integral parts of CINC plans for combined measures to be taken in the event of NBC attack. This should include the common provision of a single standard of prophylaxis across a combined force.
- Continue to develop the tactics, techniques, and procedures and the associated equipment necessary to ensure continued access for amphibious, air-delivered, and air forces in environments across the spectrum of engagement—from benign to forcible entry.

For air forces, this translates into a continual refinement and improvement of the ability to destroy or degrade enemy air defenses, particularly against a foe who chooses to employ his weapons in innovative and nontraditional ways. As Major General Bruce Carlson, USAF, has noted, "The SEAD [suppression of enemy air defenses] capability that we've built in the U.S. Air Force is a little bit dependent on the enemy fully utilizing his assets—if they're not emitting, then you're not suppressing very much."[136] Functionally, this means we need to have a "destruction" (DEAD) capability as well as a "suppression" (SEAD) capability. It also means that we need to continue to explore the technical and tactical feasibility of extreme long-range air operations, for circumstances when the threat will require distant basing.

For ground forces, the principal requirement will be the ability to conduct forcible entry operations and subsequent logistical sustainment in extremely austere environments, potentially with an extended "across the beach" or limited airhead flow of supplies for lengthy periods. The Marine Corps MV–22 and AAAV amphibian vehicle will provide the capabilities for extended-range forcible entry from across the horizon to objectives well inland, bypassing potentially defended beaches. The top-to-bottom reassessment of Army organization will yield a force that is both lighter and significantly more deployable than the current one. Aside from parachute infantry and air assault forces, how this force will integrate into forcible entry operations remains to be fully resolved, in terms of equipment, doctrine, and structure.

For naval forces, the ability to defeat the mine, cruise missile, small fast attack craft, and coastal submarine threat, and to ensure safe passage for amphibious, surface fire support, and follow-on logistics ships will be paramount.[137] Since 1950, 18 U.S. Navy ships have been damaged or sunk. Mines were responsible for 14 of these. In addition to loss of life, the cost to the nation has been many millions of dollars. The aggregate cost of the mines that caused this damage has been estimated at $11,500. Mines remain the principal threat to both warfighting and sustainment vessels, and the program of eight antimine "assigned systems" (one submarine-launched, one surface combatant-launched, and six helicopter-launched) will be critical in correcting this long-term deficiency. All joint forces must be prepared to conduct operations for extended periods of time in hazardous chemical and biological environments, and overcome this challenge through protective measures on the ground, in the air, and at sea.

In concert with industry, we need to undertake to ensure that all future military and specific civil communications and satellite systems emphasize radiation-tolerant microelectronics. This would include all satellites launched by the United States, not just military-specific systems. It is not fiscally feasible to harden all, or perhaps even military, satellites against direct (i.e., kinetic or directed energy) attack, but satellite systems can have higher levels of environmental protection designed to counter such tactics as the "pumping" of the Van Allen belt. It has been estimated that, for total programmatic costs of between 1 and 5 percent, this goal can be obtained.[138] At the same time, a *selective* retrofitting of critical U.S. theater and tactical level communications systems needs to be undertaken, with a goal of providing adequate HEMP protection for those systems. This cost will be significantly higher, reflecting the difficulty and greater expense of modifying existing systems, instead of designing protection into the system from the beginning. This could cost as much as 10 percent of each program. For this reason, this decision needs to be based on a careful study of the backbone systems necessary to execute *JV 2010* in the face of HEMP attack.

Any attempt to rejuvenate the declining radiation-tolerant microelectronics industry will require a significant government-defense industry partnership, which will have to also make it financially attractive for nonmilitary satellites to incorporate hardening principles into their design. This will not be cheap, since hardening requires both new

electronics and additional weight—both are premium in a system that will be launched into space.

While the interagency process for dealing with the consequences of mass catastrophic terrorism in the United States has been refined and improved with the establishment of a central coordinator within the White House, particular emphasis needs to be placed on the nature of the support DOD will provide in such an event from an interagency perspective. This is particularly important regarding the utilization of low-density, high-demand units and equipment in the Guard, Reserve, and Active Components, units such as chemical decontamination units and medical support elements that might be needed for simultaneous contingencies outside of the United States. This will require DOD to come to a clear and explicit understanding of how it will support the civilian government when faced with a catastrophic attack on the United States. It seems only reasonable to expect that the time of greatest danger for an attack on the continental United States might be during a significant international crisis in which many of our forces are deployed abroad. In this instance, worst-case planning is prudent.

The Department of Defense should begin this process by ensuring that all theater contingency plans are thoroughly coordinated through the Joint Staff and potential dual claims (between theater CINCs and homeland defense) on low-density, high-demand assets and stored equipment and supplies unique to catastrophic management are deconflicted and prioritized. Associated risks should be assessed and articulated, and this deconfliction, prioritization, and risk assessment should be understood at the interagency level.

We should be red teaming our own capabilities so that we have an accurate net assessment of our strengths and weaknesses. This is an effort that is important enough to have both protection and continuity, and it needs to be located outside the intelligence community, although it must have strong ties to it. For such an organization to have credibility, it must possess not only analytic capabilities, but also operational respectability—it must be staffed with operators as well as analysts. It must also have access, and access means high-level sponsorship. There is a need for this concept at every level of the Department of Defense: the services, the Joint Staff, and in the combatant commands. On the Joint Staff such an organization would be charged with review of plans and operational concepts from an adversarial, intelligence-based, and operationally validated perspective as well as other taskings from the Chairman. In time,

parallel organizations might prove useful within each regional and functional combatant command. The services have strong vested interests in looking ahead at alternative futures, and in continually refining their Title X (USC) responsibilities.

Specific Actions to Prevent Disproportionate Effect

Last, it has been argued throughout this analysis that the ultimate goal of any asymmetric approach is to seek strategic effect against the will of the opponent. This can be achieved through deterrence or coercion, or—once battle is joined—through such approaches as warrior tactics and battlespace selection. While every action recommended to this point will tend to contribute to the reduction of this effect, the most important step that can be taken in this regard is to explain clearly to the American people the purpose of an operation. While it has become conventional wisdom in some circles that the people of the United States will not accept even minimal casualties in military operations far from home, the truth is actually more complex. In fact, it seems likely that if the goals and objectives of American involvement in operations abroad are clearly and explicitly explained, support at home will be both broad and deep.

What does this mean? Telling the American people *what* we are doing when their fighting men and women are in harm's way, and *why* they are there will be ever more important in a world in which the hierarchy of information is flattening. Other advocates, perhaps unfriendly to our interests, will also be telling their side of the story. We must take advantage of every opportunity made possible by our vast information system of systems to explain what we are doing, and we must do it better than our potential opponents.

An Option of Difficulties?

This chapter answers the question posed at the beginning of this paper: *what can we do to counter asymmetric threats?* The proposals outlined above argue for both the continuation and refinement of existing programs, and in some cases for the adoption of new ones. Some have obvious benefits, but will require presidential decision (i.e., the deployment of a NMD), because of the larger political and diplomatic consequences. Some will require the breaking of long-held paradigms (i.e., the role of the National Guard). These will be difficult choices.

The recommendations having the greatest fiscal impact involve the fielding of both national and theater ballistic missile systems. While significant sums have been spent and are now currently programmed, a

decision to deploy a NMD will require significant future commitment of resources. Of lesser but still significant fiscal impact is the recommendation to improve and protect our information architecture from HEMP, and a potential restructuring of the Army National Guard for consequence management. The single recommendation having the greatest potential domestic political volatility is the recommendation to re-tool elements of the Army National Guard to better face the domestic consequence management threat, and to shift away from its current emphasis on large-scale deployments from the United States in support of theater war plans.

The objective of these recommendations is to gain the best relative competitive advantage for our nation at the least cost—in human life and national treasure—in a strategic environment in which our interest in any given engagement may not be as great as our adversary's. In preparing for this environment, it is important that we do not design our responses so narrowly that we become prisoners of our own actions. For that reason, these recommendations have sought to fulfill a basic responsibility of civil government—the protection of its citizens and their property—without becoming fixated on the defense of the United States homeland as the beginning and end of the asymmetric threat. Such an approach would entail passivity, and passivity is not in the American character. The dual objectives of protecting our citizens at home while advancing American interests abroad form the most effective possible response to asymmetric threats. We must do both. These recommendations will help us do them better.

Chapter Six

Conclusions: The Uneasy Athenians

The idea that weaker states or nonstate actors will attempt to find innovative ways to compensate for their inferiority is the basis for asymmetry. Against Athens, Melos was unable to find a way to compensate for its aggregate inferiority. The lesson of Melian failure has not lost its haunting immediacy in the retelling down through the centuries, and potential enemies of the United States may well see themselves as latter-day Melians, just as we are cast as modern Athenians. Since it will be difficult to challenge the United States directly, our opponents will seek to find our vulnerabilities, and will ruthlessly exploit them.

The first task of this paper was to define asymmetry, building upon the existing body of current definitions. A new definition was proposed, one that emphasized the psychological components and disproportionate effects of asymmetric warfare. Expanding on this definition, six recurring themes were identified that gave structure to the working definition. The basic theme was that asymmetric options flourish for the weaker party when there is a disparity of interest between the two antagonists. The target of all asymmetric approaches is the will of the opponent, and this is achieved through the pursuit of psychological effect on the strategic level, regardless of the level of war on which the asymmetric approach is employed. Each of these concepts was illuminated by an historical example, because historical and operational context is vitally important in understanding asymmetric warfare.

The second task of this paper was to determine what the asymmetric threats are to the United States and to come to a judgment on what we should concentrate on in defense planning. This required establishing a broad typology of asymmetry. Six threats were identified: nuclear, chemical, biological, information operations, alternative operational concepts, and terrorism. Each of these was examined in depth, across the

strategic, operational, and tactical levels of war. Following this, the nature of United States conventional military superiority was examined for potential vulnerabilities. The same process was applied to the critical infrastructures that provide basic services in the United States. The integration of asymmetric threats and our potential vulnerabilities enabled the creation of a list of the most serious asymmetric threats to the United States. The establishment of such a set of potential threats gives discipline to the planning process, and allows for the design of appropriate counters. Without this assessment of what is truly threatening, and what is not,it is difficult to craft a coordinated plan.

The final task of this paper was to give advice on what we need to do to improve our ability to counter asymmetric approaches. This began by evaluating the current status of existing initiatives and by making some frank judgments about where improvement is needed. The principal criticism of our current approach to the asymmetric threat is that, since we do not have a single accepted concept for how to organize for asymmetric defense, there is little coordination between existing initiatives. A top-down, simple, and clear concept is the starting point, based on three imperatives: minimize our vulnerabilities, accentuate our unique strengths, and prevent disproportionate effect. Based on these three organizing ideas, recommendations were made that would attempt to prevent another Mogadishu and deter another Pearl Harbor.

At the beginning of a new millennium, the United States is ubiquitous, and ubiquity brings vulnerability. We will be most effective in this confusing world by realizing that only former great powers have seen the end of asymmetric threats. If we are the Athenians, then we should be uneasy Athenians and remember that, while the Melians eventually succumbed to Athenian power, they did not possess the asymmetric options available to today's potential adversaries. In time, the Athenians, too, passed from the stage because they could not adapt to new strategic challenges. Today sheep graze and children play among the broken walls of Piraeus, the imperial port of once-mighty Athens.

Endnotes

[1] Thucydides, *The Landmark Thucydides,A Comprehensive Guide to the Peloponnesian War*, ed. Robert B. Strassler, trans. Richard Crawley (New York: Free Press, 1996), 352.

[2] For the purpose of this study, Alaska, Hawaii,and U.S. territories and mandates are explicitly considered to be part of the homeland.

[3] Henry A. Kissinger, *Nuclear Weapons and Foreign* Policy (New York: Council on Foreign Relations, 1957).

[4] Although the Commission on Roles and Missions identified combating proliferation of weapons of mass destruction, information warfare, peace operations,and operations other than war (OOTW) as emerging mission priorities. See *Directions for Defense: Report of the Commission on Roles and Missions of the Armed Forces*, by John P. White, Chairman, and members of the Commission on Roles and Missions of the Armed Forces (Washington, D.C.: Department of Defense, May 24,1995), ES–4.

[5] William S. Cohen, *Report of the Quadrennial Defense Review* (Washington, D.C.: Department of Defense, May 1997). See also Bruce W. Bennett et al., "What Are Asymmetric Strategies?" Documented Briefing prepared for the Office of the Secretary of Defense; delivered to the Quadrennial Defense Review Team, 1997.

[6] *Transforming Defense: National Security in the 21st Century; Report of the National Defense Panel*, by Philip A. Odeen, Chairman, and members of the National Defense Panel (Arlington, VA: National Defense Panel, December 1997); and *New World Coming: American Security in the 21st Century* (Washington, D.C.: United States Commission on National Security/21st Century, September 14, 1999).

[7] *Strategic Assessment 1998: Engaging Power for Peace* (Washington, D.C.: Institute for National Strategic Studies, National Defense University, 1998), and William S. Cohen, *Annual Report to the President and the Congress* (Washington, D.C.: Department of Defense, 1999).

[8] *A National Security Strategy for a New Century*, by William J. Clinton (Washington, D.C.: The White House,1998),and *National Military Strategy of the United States of America*, by General Henry H. Shelton (Washington, D.C.: Department of Defense, 1997).

[9] The Joint Strategy Review (JSR) is prepared each year by the Joint Staff as part of the formal strategy development and planning process within the Department of Defense.

[10] Cohen, *Annual Report to the President*, 2.

[11] Extracted from an internal briefing for the Joint Staff in June 1998.

[12] Clinton, *A National Security Strategy for a New Century*, 26.

[13] Martin van Creveld, *The Sword and the Olive: A Critical History of the Israeli Defense Force* (New York: Public Affairs, 1998), 62.

[14] This observation was offered by W. Seth Carus of the Center for Counterproliferation Research at the National Defense University. The examples of Pearl Harbor and Mogadishu, of course, are at the distant poles of the argument. Both will be discussed in this chapter.

[15] Some particularly insightful analysis on this subject has been done by Dr. Bruce Bennett of RAND Corporation and is incorporated in his unpublished brief: "Establishing a Baseline for New Force Planning Constructs: Comparing Analysis of QDR 1997." The author received this brief in October 1999.

[16] See John L. Hirsch and Robert B. Oakley, *Somalia and Operation Restore Hope*: *Reflections on Peacemaking and Peacekeeping* (Washington, D.C.: United States Institute of Peace Press, 1995), 121–125,and Keith B. Richburg, "In War on Aideed,UN Battled Itself, *The Washington Post*, December 6, 1993, 1.

[17] A good summary of this, while somewhat dated,is Louis Morton,"Japan's Decision for War," in *Command Decisions*, ed.K.R. Greenfield (Washington, D.C.: U.S. Army Center of Military History, 1990),99–124. See also David C. Evans and Mark R. Peattie, Kaigun: *Strategy, Tactics,and Technology in the Imperial Japanese Navy 1887–1941* (Annapolis, MD: Naval Institute Press, 1997), Chapter 13, "The Great Gamble."

[18] Carl von Clausewitz, *On War* (Princeton, NJ: Princeton University Press, 1984), 75.

[19] Winston Churchill, *The World Crisis: 1918–1928,The Aftermath* (New York:Scribner's,1923), 63. See also Michael Pearson, *The Sealed Train* (New York: G.P. Putnam's Sons, 1975), 64.

[20] Pearson, *The Sealed Train*, 64.

[21] This discussion is based on Richard B. Frank, *Downfall: The End of the Imperial Japanese Em - pire* (New York: Random House, 1999), 188–191, and more generally on Chapters 12 and 13: "Kamikazes, Civilians, and Assessments," and "The Eclipse of Olympic."

[22] Ibid., 182.

[23] Ibid., 186–187.

[24] See George P. Schulz, *Turmoil and Triumph: My Years as Secretary of State* (New York: Charles Scribners Sons, 1993), 227–234.

[25] Rebecca Grant, *The Kosovo Campaign: Aerospace Power Made It Work* (Arlington, VA: Air Force Association, September 1999), 15.

[26] Ibid., 16.

[27] Evans and Peattie, Kaigun, 129–131.

[28] Ibid., 268–271.

[29] Shimon Naveh, *In Pursuit of Military Excellence: The Evolution of Operational Theory* (Portland,OR: Frank Cass, 1997),16.Shock is obtainable on all three levels of war: strategic, operational, and tactical. Soviet theory teaches that there are three elements to its practice, beginning with the identification of the elements of the center of gravity: exact points of strength and weakness; deliberate creation of vulnerabilities; and exploitation of these vulnerabilities. In conventional military thinking, in the West this can be caused by a "turning maneuver," or in Soviet doctrine a "turning over," or *obkhod*. "When such conditions are realized,the opposing system is forced into a situation in which it will lose its abilities both to accomplish its original aim,and to regain its operational equilibrium."

[30] Robert Mikesh, *Japan's World War II Balloon Bomb Attacks on North America* (Washington, D.C.: Smithsonian Institution Press, 1973).

[31] The concept of a state's "strategic personality"is well articulated in R. D. Blackwill and A. B. Carter, "The Role of Intelligence," in R. D. Blackwill et al., *New Nuclear Nations: Consequences for U.S. Policy* (New York: Council on Foreign Relation Press, 1993), 217 and 236–237. Although tied to the nuclear issue, the concept has wider applicability as well.

[32] For the best general discussion of this,see James S. Corum, *The Roots of Blitzkrieg: Hans von Seekt and German Military Reform* (Lawrence, KS: University Press of Kansas, 1992).

[33] Evans and Peattie, Kaigun, 130–131.

[34] Craig R. Whitney, "Anxious French Mutter as U.S.Envoy Tries to Sell Globalization," *The New York Times*, December 2, 1999, A–12.

[35] M.A. Palmer, *Guardians of the Gulf: A History of America's Expanding Role in the Persian Gulf: 1833–1992* (New York: Free Press,1992), 120. Chapters 6,"Not while this President Serves: The Reagan Administration and the Gulf, 1981–1987," and 7, "The Tanker War, 1987–1988," form the basis for much of this analysis.

[36] Ibid., 120–121.

[37] Ibid., 130.

[38] Ibid., 131.

[39] Ibid., 135–136: No mine countermeasures vessels were on hand in the Gulf the day the *Bridgeton* was struck.

[40] The Iraqis launched 88 attacks on ships in 1987 and the Iranians launched 91. Ronald O'Rourke, "The Tanker War," *U.S. Naval Institute Proceedings* 114 (May 1988): 32.

[41] Palmer, *Guardians of the Gulf*, 144.

[42] Ibid., 147–149, and Robin Wright, *In the Name of God: The Khomeini Decade* (New York: Simon and Schuster, 1989), 183–188.

[43] From Robert G. Joseph and John F. Reichart, *Deterrence and Defense in a Nuclear, Biological, and Chemical Environment*, Occasional Paper of the Center for Counterproliferation Research (Washington, D.C.: National Defense University, Institute for National Strategic Studies, 1995), 4.

[44] *Strategic Assessment 1999*, 96. Also, see the dated but still very useful Graham T. Allison et al., *Avoiding Nuclear Anarchy: Containing the Threat of Loose Russian Nuclear Weapons and Fissile Material*, CSIA Studies in International Security #12 (Cambridge, MA: MIT Press, 1996), 28.

[45] See R.A. Falkenrath et al., *America's Achilles' Heel: Nuclear, Biological,and Chemical Terrorism and Covert Attack* (Cambridge,MA: MIT Press and the JFK School of Government, 1999), for a good summary of "who has what," based on a synthesis of unclassified sources.

[46] It is my position that this is the far more likely scenario for use. For purposes of organization, though, this has been grouped under the operational level.

[47] With one exception: the strategic deployment system has critical nodes that could be degraded through nuclear attack: ports,airfields, marshaling areas, and key bridges and transportation infrastructure.

[48] Martin van Creveld, "The Fate of the State," *Parameters* 26, no. 1 (Spring 1996): 17.

[49] Falkenrath, *America's Achilles' Heel*, 91, 226–227.

[50] Ibid., 71.

[51] Ibid., 64.

[52] Ibid., 19–26.

[53] See U.S. Congress, Office of Technology Assessment, *Technologies Underlying Weapons of Mass Destruction*, OTA–BP–ISC–115 (Washington, D.C.: Government Printing Office, 1993), 77–81 and throughout for an excellent discussion.

[54] Ibid., 77–81 and throughout for an excellent discussion.

[55] It has been asserted, in particular, that the former Soviet Union viewed contagiousness as a desirable characteristic of biological weapons, and sought to increase the contagiousness of its biological weapons accordingly.

[56] Office of Technology Assessment, *Technologies*, 77.

[57] Falkenrath, *America's Achilles' Heel*, 67.

[58] Ibid., 67–68.

[59] Ibid., 67.

[60] Ibid.

[61] See R. J. Larsen and R. P. Kadlec., *Biological Warfare: A Post Cold War Threat to America's Strategic Mobility Forces* (Pittsburgh, PA: Matthew B. Ridgway Center for International Security Studies, University of Pittsburgh, 1995), 12 and throughout for an excellent discussion of the strategic mobility threat posed by these weapons.

[62] Falkenrath, *America's Achilles' Heel*, 46–59.

[63] Office of Technology Assessment, *Technologies*, 8.

[64] Henry H. Shelton, *Information Operations: A Strategy for Peace, The Decisive Edge in War* (Washington, D.C.: The Joint Chiefs of Staff, 1999).

[65] Two recent survey works on the current state of information operations are: Zalmay Khalilzad and John P. White, eds., *The Changing Role of Information in Warfare* (Santa Monica, CA: RAND, 1999),and John Arquilla and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, CA: RAND, 1997).

[66] For a discussion of the al Firdos bunker, see Williamson Murray, *Air War in the Persian Gulf* (Baltimore, MD: Nautical and Aviation Publishing Company of America, 1995), 190.

[67] Bob Brewin,"Pentagon Hit by 'World Wide Wait,'" *Federal Computer Week*, November 15, 1999, 1.

[68] Anthony Cave Brown, *"C": The Secret Life of Sir Stewart Graham Menzies, Spymaster to Winston Churchill* (New York: Macmillan, 1987), 278.

[69] Robert T. Marsh et al., *Critical Foundations: Protecting America's Infrastructures: The Report of the President's Commission on Critical Infrastructure Protection* (Washington, D.C.: The President's Commission on Infrastructure Protection, 1997). Hereafter referred to as the *Marsh Report*.

[70] Discussion in this section is largely based on Samuel Glasstone and Philip J. Dolan, eds., *The Effects of Nuclear Weapons*, 3rd ed. (Washington, D.C.: Department of Defense, 1977), Chapters X, "Radar and Radio Effects," and XI, "The Electromagnetic Pulse and its Effects," and S.J. McGrath, "The Electromagnetic Pulse Environment and Its Influence on Tactical Electronic and Communications Equipment," Unpublished thesis for MS in Telecommunications, Naval Postgraduate School, Coronado, CA, March 1992.

[71] Glasstone and Dolan, *Effects of Nuclear Weapons*, 515.

[72] Ibid., 518.

[73] R.C. Webb et al., "The Commercial and Military Satellite Survivability Crisis," *Defense Electronics*, August 1995, 24. See also Martin Libicki, *Illuminating Tomorrow's War*, McNair Paper 61 (Washington, D.C.: National Defense University, Institute for National Strategic Studies, October 1999), 14: "The few really good eyes in the U.S. space inventory may be vulnerable to attack."

[74] Webb, "The Commercial and Military Satellite Survivability Crisis," 24.

[75] See Andrew Koch, "Interview: Dr. Jay Davis, Director of the U.S. Defense Threat Reduction Agency (DTRA)," *Jane's Defence Weekly*, February 16, 2000, 32: "An EMP attack 'is technically quite simple to do with a relatively crude nuclear weapon,' he adds. 'If you look at the effects of that on our communications and telecommunications systems, and if you look at the more problematic effect of EMP from a high-altitude burst over US forces or over part of the USA, it becomes an attractive equalizer for a less sophisticated military opponent or even a terrorist.'"

[76] Glasstone and Dolan, *Effects of Nuclear Weapons*, 520–532.

[77] Norman Friedman, "Russians Offer EMP Counter," *U.S. Naval Institute Proceedings* 123 (August 1997): 91–92.

[78] See Bruce D. Nordwell, "EMP, High-Powered Microwaves Pose New EW Threat to Aircraft," *Aviation Week and Space Technology*, October 26, 1998, 68.

[79] Webb, "The Commercial and Military Satellite Survivability Crisis," 21.

[80] Testimony of Mr. Gil I. Klinger (Acting Deputy Under Secretary of Defense for Space) to the House National Security Subcommittee on Military Research and Development, July 16, 1997, Y4.SE2/1 A:997–98/18, 5.

[81] Testimony of Dr. Lowell Wood (Visiting Fellow, Hoover Institution on War, Revolution, and Peace, Stanford University, Stanford, CA) to the House National Security Subcommittee on Military Research and Development, July 16, 1997, Y4.SE2/1 A:997–98/18, 5.

[82] Ibid.

[83] Quoted in Daniel Verton, "Army Battles Irrelevancy," *Federal Computer Week*, November 15, 1999, 10.

[84] Sha Lin, "Two Senior Colonels and No-Limit War," *Beijing Zhongguo Qingnian Bao* in Chinese, June 28, 1999, 5 (Foreign Broadcast Information Service translation).

[85] See Charles J. Dunlap, "21st Century Land Warfare: Four Dangerous Myths," *Landpower in the 21st Century: Preparing for Conflict* (Carlisle, PA: U.S. Army War College, April 1998), 83–93, for a good analysis of this.

[86] For a broad sampling of Chinese thinking in this area, see Michael Pillsbury, *China Debates the Future Security Environment* (Washington, D.C.: National Defense University Press, 2000), and Michael Pillsbury, ed., *Chinese Views of Future Warfare* (Washington, D.C.: National Defense University Press, 1997).

[87] See also Fred Kennedy et al., "A Failure of Vision," *Airpower Journal* (Summer 1998): 84–94.

[88] P. D. Feaver, and C. Gelpi, "How Many Deaths Are Acceptable? A Surprising Answer," *The Washington Post*, November 7, 1999, B–3, which describes the results of the Triangle Institute for Security Studies (TISS) Casualty Aversion Survey, conducted during the period September 1998 through June 1999.

[89] This term was used in a brief the author received at Headquarters, Task Force *Eagle*, 1st Cavalry Division, Tuzla, Bosnia, January 1999.

[90] Harry G. Summers, Jr., *On Strategy: A Critical Analysis of the Vietnam War* (Novato, CA: Presidio, 1982), 1.

[91] Clausewitz, *On War*, 77.

[92] See Libicki, *Illuminating Tomorrow's War*, 47–50 for a thoughtful discussion of this problem.

[93] See Gerald Segal, "Does China Matter?" *Foreign Affairs* 78, no. 5 (September/October 1999): 30, for an analysis of the effect of China's nuclear force on U.S. strategic calculations.

[94] See Edward N. Luttwak, "A Post-Heroic Military Policy," *Foreign Affairs* 75, no. 4 (July/August 1996): 33–44, for a presentation of this view.

[95] For example, Benjamin C.Schwarz, *Casualties: Public Opinion and U.S. Military Intervention* (Santa Monica, CA: RAND, 1994), finds that U.S. casualties might actually increase the will of the American people to pursue victory instead of withdrawal.

[96] Robert W. Chandler, *Tomorrow's War, Today's Decisions* (McLean, VA: AMCODA Press, 1996). See also Greg Weaver and D. J. Glaes, *Inviting Disaster: How Weapons of Mass Destruction Undermine U.S. Strategy for Projecting Military Power* (Mclean, VA: AMCODA Press, undated). Also in this camp is Paul Bracken, *Fire in the East: The Rise of Asian Military Power and the Second Nuclear Age* (New York: HarperCollins Publishers, 1999).

[97] Robert H.Scales,Jr., "The Indirect Approach: How U.S. Military Forces Can Avoid the Pitfalls of Urban Warfare," in *Future Warfare* (Carlisle, PA: U.S. Army War College, 1999), 173–185.

[98] See Allen Hammond, *Which World? Scenarios for the 21st Century* (Washington, D.C.: Island Press, 1998), 72–74, for a discussion of the urbanization of the world.

[99] Air power theorist John Warden argues that it may be possible to exercise crowd control in an urban environment with "a combination of AC–130s and helicopters in the air equipped with searchlights, loudspeakers, rubber bullets, entangling chemical nets, and other paraphernalia." See John Warden, "Air Theory for the Twenty-first Century," in Karl P. Magyar et al., eds., *Challenge and Response: Anticipating U.S. Military Concerns* (Maxwell Air Force Base, AL: Air University Press, 1994), 330.

[100] Paul K. Van Riper and Robert H. Scales, Jr., in "Preparing for War in the 21st Century," in *Landpower in the 21st Century: Preparing for Conflict* (Carlisle, PA: U.S. Army War College, April 1998),3–12,make the point that "In an uncertain world, we dare not base force requirements on preconceived assumptions about whom we might fight in the next century or how."

[101] And this generated the March 1942 attack on Lubeck, an unimportant north German coastal town of little strategic significance. See the Royal Air Force's Official History, by Charles Webster and Noble Frankland, vol.I, *The Strategic Air Offensive Against Germany* (London: Her Majesty's Stationary Office,1961),392. The incident "showed the extent . . . to which a town might become a target mainly because it was operationally vulnerable." See also Max Hastings, *Bomber Command* (New York: Dial Press,1979),147–148.

[102] Also known to some as a "regional near-peer" adversary or competitor.

[103] Clarke's Third Law, from Arthur C. Clarke, *Profiles of the Future: An Inquiry into the Limits of the Possible* (New York: Harper and Row, 1973), 21.

[104] Science fiction classic by Frank Herbert, *Dune* (New York: Putnam Publishing Group, 1984),409.

[105] A good discussion of the arguments surrounding the "transportation plan" is found in W. W. Rostow, *Pre-Invasion Bombing Strategy: General Eisenhower's Decision of March 25,1944* (Austin,TX: University of Texas Press, 1981). For the al Firdos bunker, see Murray, *Air War in the Persian Gulf*, 190–192.

[106] The best general discussion of this is D. S. Alberts, J. J. Garstka,and F. P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority,* 2d ed. revised (Washington, D.C.: DoD C4ISR Cooperative Research Program, 1999), 87–114, but also throughout.

[107] There are a number of sharp critiques of *JV 2010*. Two worth noting are Charles J. Dunlap, Jr., "*Joint Vision 2010:* A Red Team Assessment," and F. G. Hoffman, "*Joint Vision 2010*—A Marine Perspective," both in *Joint Force Quarterly* 17 (Autumn/Winter 1997–1998):47–49 and 32–38, respectively.

[108] Noting the significant exceptions of Pearl Harbor and the Alaskan islands in World War II.

[109] The data in this table,and many of the underpinnings of arguments developed in this section, are derived from the previously cited *Marsh Report.*

[110] Paul F. Herman, "Asymmetric Warfare: Sizing the Threat," *Low Intensity Conflict and Law Enforcement* 6, no. 1 (Summer 1997): 180. This excellent article deals clearly with the conceptual underpinnings of asymmetric warfare.

[111] A good summary of this can be found in Brad C. Roberts,"From Nonproliferation to Antiproliferation," *International Security* (Summer 1993): 158,"In the United States, proliferation is likely to sharpen the debate about vital versus peripheral national interests,undermine the political support for military intervention, or even long term engagement,increase U.S. vulnerability to coercive diplomacy by regional actors, and narrow the room for maneuver in [the] international environment."

[112] E. Anders Eriksson, "Viewpoint: Information Warfare: Hype or Reality?" *The Nonproliferation Review* 6, no. 3 (Spring/Summer 1999): 57–64.

[113] Libicki, *Defending Cyberspace and Other Metaphors*, 11–13.

[114] Based on Office of Technology Assessment, *Technologies Underlying Weapons of Mass Destruction*, 78: "One gram of dried anthrax spores contains more than 10^{11} particles; since the lethal dose by inhalation in monkeys is between 10^3 and 10^4 spores,a gram of anthrax theoretically contains some 10 million lethal doses."

[115] Webb et al., "The Commercial and Military Satellite Survivability Crisis," 22–24.

[116] The threat of a chemical attack against the homeland,although a different threat,is assumed as a "lesser included" consideration for purposes of analysis here.

[117] PDD–62,signed on May 22,1998, expands and more clearly focuses PDD–39,and "creates a new and more systematic approach to fighting the terrorist threat of the next century. It reinforces the mission of the many U.S.agencies charged with roles in defeating terrorism; it also codifies and clarifies their activities in the wide range of U.S. counter-terrorism programs from apprehension and prosecution of terrorists to increasing transportation security, enhancing response capabilities and protecting the computer-based systems that lie at the heart of America's economy." Additionally, PDD–62 established the Office of the National Coordinator for Security, Infrastructure Protection, and Counter-terrorism within the National Security Council. This information is taken from the White House,"Fact Sheet on Combating Terrorism: Presidential Decision Directive 62," May 22, 1998.

[118] PDD–39, signed on June 21, 1995,establishes broad measures to combat terrorism through reducing vulnerabilities, deterring, and responding, to include NBC consequence management. The thrust of this PDD is against terrorist attack on the homeland using WMD. Taken from PDD–39: U.S. Policy on Combating Terrorism (unclassified abstract), Chapter Report, 09/26/97,GAO/NSIAD–97–254, Appendix 1.

[119] The Nunn-Lugar-Domenici Domestic Preparedness Program was designed to increase training of potential first responders to WMD terrorist incidents within the United States. By the end of 1998, 40 U.S. cities had received training, with training ongoing in an additional 80. As part of this program, each designated city receives $300,000 from DOD for personal protection, decontamination, and detection equipment. The Public Health Service will assist in the establishment of Metropolitan Medical Strike Teams in each of the cities, at a cost of approximately $350,000 per city for equipment and pharmaceuticals. This information is taken from The Monterey Institute of International Studies, Center for Nonproliferation Studies, Chemical and Biological Weapons Resource Page, "United States response to CBW terrorism and domestic preparedness" (*http://cns.miis.edu/research/cbw/domestic.htm)*.

[120] PDD–63, signed on May 22,1998,was based on many of the recommendations of the Commission on Critical Infrastructure Protection as given in the *Marsh Report*, and called for these key steps to be taken:

—Improved interagency coordination for critical infrastructure protection

—Definition of the roles and responsibilities of U.S. agencies in fighting terrorism

—Establishment of departmental Chief Information Officers (CIOs) within the Federal Government, with responsibilities for information assurance

—Designation of the National Coordinator for Security, Infrastructure Protection and Counterterrorism as the governmental officer responsible for implementation of the provisions of PDD–63

—Improvements in capabilities for protecting the national information structure,the most important of which is the creation of a National Infrastructure Protection Center (NIPC) in the FBI

—Promotion of partnerships with industry and other private players to enhance computer security

—Study plans for minimizing damage and recovering rapidly from attacks on vital infrastructure.

See *White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, May 22, 1998 (Washington, D.C.: The White House, 1998).

[121] See the testimony of J. Stapleton Roy, Assistant Secretary of State for Intelligence and Research,in John Donnelly, "Intelligence Officials: Missiles Attack on U.S.'Unlikely,'" *Defense Week*, February 14,1. The testimony of Mr. Roy and other officials before the Senate Intelligence Committee indicated that they consider covert means of attack more likely than a direct missile attack.

[122] See James S.Gilmore et al., *First Annual Report to the President and the Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction* (Washington, D.C., December 15, 1999).

[123] JTF–CND was established December 4, 1998, with responsibility for defense of DOD networks and computer systems.

[124] Statement of Mark E. Gebicke, Director, Military Operations and Capabilities Issues, National Security and International Affairs Division, General Accounting Office, before U.S. Senate, Committee on Veteran's Affairs, March 17,1998: "Chemical and Biological Defense: Observations on DoD's Plans to Protect U.S. Forces" (GAO/T–NSIAD–98–83), p. 2. According to Mr. Gebicke, "there are deficiencies in doctrine, policy, equipment,and training for the defense of critical ports and airfields."

[125] For example, see unattributed,"Navy Mine Warfare Official Warns Judgment Day is Coming," *Inside the Navy*, November 22,1999,7. As cited herein,the Navy's mine warfare program has $5 billion budgeted against it across the future years defense plan, but at least one of the seven mine-clearing systems is being slipped.Dale Gerry, Navy Deputy Assistant Secretary for Mine and Undersea Warfare,is concerned about the Navy's ability to meet the goal of outfitting one carrier battle group with organic mine countermeasures by 2005.

[126] Two differing perspectives on this issue can be found in (for the affirmative) Henry A. Kissinger,"The Next President's First Obligation," *The Washington Post*, February 9,2000,21,and (for the negative) George Lewis,Lisbeth Gronlund,and David Wright,"National Missile Defense: An Indefensible System," *Foreign Policy* (Winter 1999–2000): 120–131.

[127] John Parachini, Center for Nonproliferation Studies, Monterey Institute of International Studies, "U.S.Government Spending to Combat Terrorism: Chart and Analysis" (*http://cns.miis.edu/research/cbw/ternarr.html*).

[128] Ibid., 2.

[129] See the Office of the Secretary of Defense, *Reserve Component Employment Study 2005, Study Report* (Washington, D.C.: Office of the Secretary of Defense, July 1999).

[130] This builds on recommendations in the *1997 Quadrennial Defense Review*, the *Reserve Component Study* completed in 1999,and the *1999 Report to the National Guard Bureau Weapons of Mass Destruction (WMD) Study* (Washington, D.C.: Science Applications International Corporation, February 1999).

[131] OSD, *Reserve Component Study*, C–1, 2. The *1999 Report to the National Guard Bureau Weapons of Mass Destruction (WMD) Study*, 4, identified 141 potential support roles for the National Guard, and then refined them to "47 mission consistent potential National Guard WMD response support roles."

[132] Here is an example of how such a restructuring might be accomplished, based on Annex C, "Missioning RC units for CM and critical infrastructure physical security," in the *Reserve Component Study* cited above. Beginning by assuming that a surge chemical decontamination capability is needed for every major metropolitan area in the United States with over 200,000 people, then the requirement will be for 76 organizations with this capability. If the unit of measure is a chemical company, then a requirement would exist for 76 chemical companies. There are 42 chemical companies in the Reserve Components, of which 9 are in the National Guard and 33 in the Army reserve. All are currently tasked under existing regional warplans. For these reasons, dual-missioning existing companies is not feasible. Developing 76 chemical companies including procurement of equipment and personnel retraining would cost in the neighborhood of $200 million.

[133] See Seymour Hersh, "The Intelligence Gap," *The New Yorker*, December 6,1999,58–67, for a discussion of the challenges facing the National Security Agency. For example, "the North Koreans . . .have bought encrypted phones from Europe,high-speed switching gear from Britain,and up-to-date dialing service from America—a system the NSA cannot readily read." A U.S."intelligence official" went on to say that "All their military stuff went off ether into fiber—from high frequency radio transmission to fiber-optic cable lines." Fiber-optic cable is both capable of carrying much more traffic than any radio transmission,and cannot be readily read by external monitoring systems. See also Douglas Farah,"New Drug Smugglers Hold Tech Advantage," *The Washington Post*, November 15, 1999, 1., which outlines some of the encryption techniques readily available to well-funded transnational criminal organizations.

[134] Falkenrath, *America's Achilles' Heel*, 282–286, makes some of these recommendations in Chapter 5,"Recommendations: An Agenda for the American Government."

[135] In the TMD arena, the Army's PAC–3 and the Navy Area Defense systems are already budgeted.

[136] Quoted in John A. Tirpak,"Dealing With Air Defenses," *Air Force Magazine*, November 1999,26.

[137] Unattributed,"Navy Mine Warfare Official Warns 'Judgment Day' Is Coming,'" *Inside the Navy*, November 22, 1999, 7.

[138] Joseph C. Anselmo, "U.S. Seen More Vulnerable to Electromagnetic Attack," *Aviation Week and Space Technology*, July 28, 1997, 67.

USGPO : 187–600

NDU Press
ATTN: NDU–NSS–PD
300 Fifth Avenue (Bldg. 62)
Fort Lesley J. McNair
Washington, D.C. 20319–5066

Telephone: (202) 685–4210
Facsimile: (202) 685–4806

About INSS Publications

Print Publications

For general information on publications and other programs of the Institute for National Strategic Studies, consult the National Defense University Web site at ***http://www.ndu.edu***. To request a complimentary copy of available NDU Press titles, contact ***ndupress@ndu.edu*** via e-mail or leave a voice message at (202) 685–4210. Most NDU Press titles can be purchased from the U.S. Government Printing Office; call (202) 512–1800 or order on-line at ***http://www.access.gpo.gov***.

Electronic Publications

Numerous titles published by NDU Press are available on line at ***http://www.ndu.edu/ndu/inss/press/ndup2.html***

Joint Force Quarterly (JFQ)

The journal publishes articles, reviews, professional notes, and other features by military officers, defense analysts, and scholars on the integrated employment of land, sea, air, space, and special operations forces. *JFQ* focuses on joint doctrine, coalition warfare, contingency planning, combat operations conducted by unified commands, and joint force development. For current and back numbers of the journal, visit the *JFQ* Home Page at ***http://www.dtic.mil/doctrine/jel/jfq_pubs/index.htm***

From the foreword to

The Revenge of the Melians

This essay is a product of the Quadrennial Defense Review (QDR) 2001 Working Group, a project of the Institute for National Strategic Studies at the National Defense University. Sponsored by the Chairman of the Joint Chiefs of Staff, the working group is an independent, honest-broker effort intended to build intellectual capital for the upcoming QDR.

One of the group's initial tasks was to assess the future security environment to the year 2025. This was pursued by surveying the available literature to identify areas of consensus and debate and by deepening knowledge of asymmetric threats to the United States both at home and abroad, given their potential appeal to likely adversaries in view of America's conventional military superiority.

Recent titles in the McNair Paper series:

61
Illuminating Tomorrow's War
Martin C. Libicki

60
The Revolution in Military Affairs: Allied Perspectives
Robbin F. Laird and Holger H. Mey

59
Right Makes Might: Freedom and Power in the Information Age
David C. Gompert

58
Searching for Partners: Regional Organizations and Peace Operations
William H. Lewis and Edward Marks

57
Modern U.S. Civil-Military Relations: Wielding the Terrible Swift Sword
David E. Johnson